2015 WL 4945713 (Pa.Com.Pl.Civil Div.) (Trial Order)
Court of Common Pleas of Pennsylvania.
Civil Division
Allegheny County

Barbara A. DITTMAN, Gary R. Douglas, Alice Pastirik, Joann Decolati, Tina Sorrentino, Kristen Cushhman, and Shannon Molyneaux, individually and on behalf of all others similarly situated, Plaintiffs,
v.
UPMC d/b/a The University of Pittsburgh Medical Center, and UPMC McKeesport, Defendants.

No. GD-14-003285.
May 28, 2015.

Opinion and Order of Court

Gary F. Lynch, Esquire, Edwin J. Kilpela, Jr., Esquire, Benjamin J. Sweet, Esquire, Jamisen A. Etzel, Esquire, Suite 210 PNC Park, 115 Federal Street, Pittsburgh, PA 15212; Michael L. Kraemer, Esquire, David M. Manes, Esquire, Elizabeth Pollock-Avery, Esquire, 600 Grant Street, Suite 660, Pittsburgh, PA 15219; Karen Hanson Riebel, Esquire, Suite 2200, 100 Washington Avenue South, Minneapolis, MN 55401-2159, Counsel for Plaintiffs.

John C. Conti, Esquire, Christopher T. Lee, Esquire, Andrew T. Tillapaugh, Esquire, Two PPG Place, Suite 400, Pittsburgh, PA 15222-5402, Counsel for Defendants.

R. Stanton Wettick, Jr., Judge.

***1** WETTICK, J.

The preliminary objections of defendants ("UPMC") seeking dismissal of both counts within plaintiffs' two-count Second Amended Class Action Complaint are the subject of this Opinion and Order of Court.

The named plaintiffs and the members of the class consist of all 62,000 UPMC employees as well as an untold number of former employees, whose names, birthdates, social security numbers, confidential tax information, addresses, salaries, and bank account information were stolen from UPMC's computer systems. The Complaint alleges that UPMC had a duty to protect the private, highly sensitive, confidential and personal financial information, and the tax documents of plaintiffs and the members of the proposed class (Second Am. Compl. ¶ 28).

Apparently to show the magnitude of the problem of thefts of confidential information, plaintiffs allege that a 2013 Identity Fraud Report released by Javelin Strategy & Research states that in 2012 identity fraud incidents increased by more than one million victims and fraudsters stole nearly $21 billion. This study found 12.6 million victims of identity fraud in the United States in the past year, which equates to one victim every three seconds. The Report also found that nearly one in four data breach letter recipients became a victim of identity fraud, with breaches involving Social Security numbers to be the most damaging (Second Am. Compl. ¶ 30).

COUNT I—NEGLIGENCE

In Count I—Negligence—plaintiffs allege that UPMC had a duty to exercise reasonable care to protect and secure its employees' personal and financial information within its possession or control from being compromised, stolen, lost, misused, and/or disclosed to unauthorized parties.

Paragraphs 52-62 of plaintiffs' negligence count read as follows:
52. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein.

53. UPMC had a duty to exercise reasonable care to protect and secure Plaintiffs' and the members of the proposed Classes' personal and financial information within its possession or control from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This highly confidential personal and financial information includes but is not limited to Social Security numbers, dates of birth, full legal names, addresses, bank account information, and other personal information.

54. UPMC's duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiffs' and the members of the proposed Classes personal and financial information in their possession was adequately secured and protected.

55. UPMC further had a duty to implement processes that would detect a breach of its security systems in a timely manner.

56. In light of the special relationship between Plaintiffs and members of the proposed Classes and UPMC, whereby UPMC required Plaintiffs and members of the proposed Classes to provide highly sensitive confidential personal and financial information as a condition of their employment, UPMC undertook a duty of care to ensure the security of such information.

***2** 57. Through its acts or omissions, UPMC breached its duty to use reasonable care to protect and secure Plaintiffs' and the members of the proposed Classes' personal and financial information within its possession or control. UPMC breached its duty by failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and members of the proposed Classes' personal and financial information, failing to adequately monitor the security of its network, allowing unauthorized access to Plaintiffs' and the members of the proposed Classes' personal and financial information, and failing to recognize in a timely manner that Plaintiffs' and members of the proposed Classes' personal and financial information had been compromised.

58. UPMC's failure to comply with widespread industry standards relating to data security, as well as the delay between the date of the intrusion and the date Plaintiffs and members of the proposed Classes were informed of the Data Breach further evidence UPMC's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and the members of the proposed Classes' personal and financial information in its possession or control.

59. But for UPMC's wrongful and negligent breach of the duties owed to Plaintiffs and the members of the proposed Classes, the Data Breach would not have occurred and Plaintiffs' and the members of the proposed Classes' personal and financial information would not have been compromised.

60. The injury and harm suffered by Plaintiffs and the members of the proposed Classes was the reasonably foreseeable and probable result of UPMC's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the members of the proposed Classes' personal and financial information in its possession or control. UPMC knew or should have known that its systems and technologies for processing and securing Plaintiffs' and members of the proposed Classes' personal and financial information had significant vulnerabilities.

61. As a result of UPMC's negligence, Plaintiffs and the members of the proposed Classes have incurred damages relating to fraudulently filed tax returns.

62. As a result of UPMC's negligence, Plaintiffs and the members of the proposed Classes are at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse.

This negligence count is based on plaintiffs' contention that UPMC owed a duty of care to UPMC employees who were victims of third-party criminal activity. However, the only losses that the UPMC employees sustained are economic losses. Under the economic loss doctrine, no cause of action exists for negligence that results solely in economic losses unaccompanied by physical injury or property damage. *Excavation Technologies, Inc. v. Columbia Gas Co. of Pa.*, 985 A.2d 840, 841 (Pa. 2009); *Adams v. Copper Beach Townhome Communities, LP.*, 816 A.2d 301 (Pa. Super. 2003).

Bilt-Rite Contractors, Inc. v. The Architectural Studio, 866 A.2d 270 (Pa. 2005), does not apply because, as explained in the Supreme Court's Opinion in *Excavation Technologies* at 843, *Bilt-Rite* served to "clarify the elements of the tort as they apply to those in the business of supplying information to others for pecuniary gain." *Id.* at 843, quoting *Bilt-Rite* at 280. See *Sovereign Bank v. B.J.'s Wholesale Club, Inc.*, 533 F.3d 162, 177-78 (3d Cir. 2008) ("The Pennsylvania Supreme Court [in *Bilt-Rite*] never suggested that it intended to severely weaken or undermine the economic loss doctrine in a case such as this. It simply carved out a narrow exception when losses result from the reliance on the advice of professionals.").

The present case does not involve defendants in the business of supplying information for economic gain.

***3** Plaintiffs contend that a duty of care should be imposed on UPMC to protect the confidential information of its employees. Plaintiffs rely on Pennsylvania Supreme Court case law (most recently *Seebold v. Prison Health Servs., Inc.*, 57 A.3d 1232 (Pa. 2012)), discussing the factors a court should consider in determining whether to impose a duty of care:

> The common pleas court sustained PHS's preliminary objections based on the no-duty contention. Initially, the court recited that, in determining whether a defendant owes a duty of care to a plaintiff, several factors are considered, including: (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. *See Seebold v. Prison Health Servs., Inc.*, No. 07-00024, *slip op.* at 2 (C.P. Lycoming, Dec. 4, 2008) (citing *Althaus v. Cohen*, 562 Pa. 547, 553, 756 A.2d 1166, 1169 (2000)).

Seebold, at 1234.

Where only economic losses are involved, the Pennsylvania appellate courts have already balanced the competing interests through the adoption of the economic loss doctrine. Thus, the *Seebold/Althaus* factors should not be considered where the plaintiff seeks to recover only economic losses.

Moreover, even when I consider the factors described in *Seebold/Althaus*, I do not find that the courts should impose a new affirmative duty of care that would allow data breach actions to recover damages recognized in common law negligence actions.

In the fact situation in which a person's confidential information was made available to third persons through a data breach, I find that the controlling factors are the consequences of imposing a duty upon the actor and the overall public interest in the proposed solution. Plaintiffs' proposed solution is the creation of a private negligence cause of action to recover actual damages, including damages for increased risks, upon a showing that the plaintiff's confidential information was made available to third persons through a data breach.

The public interest is not furthered by this proposed solution. Data breaches are widespread. They frequently occur because of sophisticated criminal activity of third persons. There is not a safe harbor for entities storing confidential information.

The creation of a private cause of action could result within Pennsylvania alone of the filing each year of possibly hundreds of thousands of lawsuits by persons whose confidential information may be in the hands of third persons. Clearly, the judicial system is not equipped to handle this increased caseload of negligence actions. Courts will not adopt a proposed solution that will overwhelm Pennsylvania's judicial system.

Also, assuming that liability is not absolute, there are not any generally accepted reasonable care standards. Use of "expert" testimony and jury findings to develop standards as to what constitutes reasonable care is not a viable method for resolving the difficult issue of the minimum requirements of care that should be imposed in data breach litigation, assuming that any minimum requirements should be imposed.

Under plaintiffs' proposed solution, in Pennsylvania alone, perhaps hundreds of profit and nonprofit entities would be required to expend substantial resources responding to the resulting lawsuits. These entities are victims of the same criminal activity as the plaintiffs. The courts should not, without guidance from the Legislature, create a body of law that does not allow entities that are victims of criminal activity to get on with their businesses.

***4** In *Seebold*, the Pennsylvania Supreme Court stated that more is involved in a court's decision as to whether to create a new duty than considering the five *Seebold/Althaus* factors. The *Seebold* Opinion stated: "To the extent that the task of rendering duty versus no-duty decisions continues to reside with jurists, we acknowledge that it is one to which we are the least well suited." *Id.* at 1245. "[W]e have often recognized the superior tools and resources available to the Legislature in making social policy judgments, including comprehensive investigations and policy hearings." *Id.* Thus, the five factors should be considered in the context of court rulings adopting "the default position that, unless the justifications for and consequences of judicial policymaking are reasonably clear with the balance of factors favorably predominating, we will not impose new affirmative duties." *Id.* "Before a change in the law is made, a court, if it is to act responsibly must be able to see with reasonable clarity the results of its decision and to say with reasonable certainty that the change will serve the best interests of society." *Id.*, quoting *Hoven v. Kelble*, 256 N.W.2d 379, 392 (Wis. 1977). See also *Lance v. Wyeth*, 85 A.3d 434, 454 (Pa. 2014).

I cannot say with reasonable certainty that the best interests of society would be served through the recognition of new affirmative duties of care imposing liability on health care providers and other entities electronically storing confidential information, the financial impact of which could even put these entities out of business. Entities storing confidential information already have an incentive to protect confidential information because any breach will affect their operations. An "improved" system for storing confidential information will not necessarily prevent a breach of the system. These entities are also victims of criminal activity.

It is appropriate for courts to consider the creation of a new duty where what the court is considering is sufficiently narrow that it is not on the radar screen of the Legislature. In that situation, the courts are filling gaps that are not likely to be filled by the Legislature. However, where the Legislature is already considering what courts are being asked to consider, in the absence of constitutional issues, courts must defer to the Legislature.

The Legislature is aware of and has considered the issues that plaintiffs want this court to consider. As of this date, the only legislation which the General Assembly has chosen to enact requires entities that suffer a breach of their security systems to provide notification. Furthermore, the Legislature gives the Office of Attorney General exclusive authority to bring an action for violation of the notification requirement (i.e., no private actions are permitted).

See pages 14-15 set forth below of UPMC's Supplemental Brief in Support of Preliminary Objections, which describe the General Assembly's consideration of data breaches:

2. The General Assembly has considered the creation of civil liability for data breaches and decided against the imposition of such a duty.

The Pennsylvania General Assembly extensively considered data breaches and the issues related thereto prior to enacting the Breach of Personal Information Notification Act (the "Data Breach Act"). 73 P.S. § 2301, *et seq.* (effective June 20, 2006). Ultimately, the General Assembly **did not, by way of the Data Breach Act, enact legislation establishing a duty of protection or providing individuals with a private cause of action** in the event of a data breach. Instead, the General Assembly mandated **only** that entities which suffer a "breach of the security of the system" must provide ***notification*** of the disclosure of personal information. See 73 P.S. § 2303 ("Any entity that maintains, store or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach …").

In the Data Breach Act, the General Assembly also established an enforcement action - expressly reserved for the Attorney General of Pennsylvania - for violation of the notification requirement. 73 P.S. § 2308 ("The Office of Attorney General shall have exclusive authority to bring an action ...."). Significantly, the General Assembly did not adopt or establish (1) a duty to protect or safeguard the security of computerized data against malicious and criminal attacks by third parties or (2) a cause of action for private litigants in the event of unauthorized access to the individuals' personal information.

***5** Indeed, review of the legislative history of Pennsylvania's Data Breach Act reveals that the General Assembly considered incorporating an expansive civil liability provision, which would have permitted a person to recover "actual damages." S.B. 712, Printer's No. 859, § 8. The initial version of the bill was referred to the Communications and Technology Committee on June 3, 2005. History of S.B. 712 of 2005. Thereafter, on June 13, 2005, the bill was reported as amended by committee and the "Civil Relief provision was amended to reflect its current form. S.B. 712, Printer's No. 898, § 8. [2] **Under its current form, only a failure to notify is actionable and only the Attorney General may assert the claim.** 73 P.S. § 2308.

(Emphasis in original.)

In summary, the General Assembly has considered and continues to consider the same issues that plaintiffs are requesting this 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 Legislature.

I find to be persuasive the Opinion of an Illinois appellate court in *Cooney v. Chicago Pub. Sch.*, 943 N.E.2d 23, 28-29 (III. App. Ct. 2010), which rejected the plaintiffs' request that the court create a new common law duty to protect and safeguard confidential information because the Legislature 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 [defendantl to provide notice of the disclosure.***

Cooney, 943 N.E.2d at 29 (emphasis added).

For these reasons, I dismiss Count I of plaintiffs' Complaint.

COUNT II—BREACH OF CONTRACT

I now consider defendants' preliminary objections seeking dismissal of Count II— Breach of Contract.

Plaintiffs contend that the relationship between plaintiffs and UPMC is governed by an implied contract. Under the terms of this implied contract, plaintiffs have agreed to make their personal information available to UPMC and UPMC has agreed "to protect the security of such information" (Second Am. Compl. ¶ 64). This implied contract requires "UPMC to safeguard and protect Plaintiffs' and the members of the proposed Classes' personal and financial information from being compromised and/or stolen" (Second Am. Compl. ¶ 66). Plaintiffs allege that "UPMC did not safeguard or protect Plaintiffs' and the proposed Class members' personal and financial information from being accessed, compromised, and/or stolen. UPMC did not maintain sufficient security measures and procedures to prevent unauthorized access to Plaintiffs' and the proposed Class members' personal and financial information" (Second Am. Compl. ¶ 67). "Because UPMC failed to safeguard and/or protect Plaintiffs' and the proposed Class members' personal and financial information from being compromised or stolen, UPMC breach[ed] its contracts with Plaintiffs and the members of the proposed Classes" (Second Am. Compl. ¶ 68).

***6** For there to be an implied contract, there must be a meeting of the minds. *Restatement (Second) of Contracts*, § 4. An implied contract is not an agreement imposed on parties to achieve justice.

In this case, there is no evidence that there has been any meeting of the minds.

Plaintiffs' Complaint does not describe an agreement between the parties. Plaintiffs do not describe any exchanges between plaintiffs and UPMC in which UPMC made any promises.

UPMC requires its employees to furnish confidential information needed in order for the employees to be paid and for UPMC to comply with governmental reporting requirements. There is no apparent reason why UPMC would enter into an agreement with its employees to allow its employees to sue UPMC in the event of a data breach. To the contrary, UPMC would anticipate that it is likely to experience data breaches, and common sense requires a finding that it would not agree to allow others to bring private actions against UPMC.

In summary, I am dismissing Count II because there are no factual allegations supporting a finding of an agreement between the parties under which UPMC agreed to be liable to its employees for criminal acts of third parties. While an implied contract may be found to exist "where the surrounding circumstances support a demonstrated intent to contract" (*Tyco Electronics Corp. v. Davis*, 895 A.2d 638, 640 (Pa. Super. 2006)), in this case, there are no circumstances that would establish a common understanding that UPMC was agreeing to allow its employees to sue UPMC for damages sustained from a data breach.

For these reasons, I enter the following Order of Court:

ORDER OF COURT

On this *28* day of May, 2015, it is hereby ORDERED that defendants' preliminary objections are sustained, and both counts within plaintiffs' Second Amended Class Action Complaint are dismissed.

BY THE COURT:

<<signature>>

WETTICK, J.

Footnotes

2 Numerous iterations of the law were proposed in the House of Representatives and the Senate, some of which provided an even more expansive array of damages to individuals victimized by data breaches. For example, H.B. 2006 of the 2005-2006 session of the Genera) Assembly provided for the award of actual damages and a fine of up to $150,000.00. H.B. 2006, Printer's No. 2925. The General Assembly chose by collective action, however, to enact a version without such provisions.