VOLUME 8, ISSUE 1

PROFESSIONAL LIABILITY DEFENSE QUARTERLY

WINTER 2016

## ANOTHER DATA BREACH DEFENSE: ECONOMIC LOSS DOCTRINE

BY: ANTHONY S. COTTONE, ESQ.

If you can remember back to the blustery winds of early October in Chicago, while we all gathered last year for the Annual PLDF Conference, you may remember a presentation during the break-out sessions on Data Breach Litigation and Cyber Security. You might also remember hearing about three theories of defense to the most common data breach cases: absence of Article III standing to bring suit in federal court, challenging class certification, and attacking hard-to-prove damages claims. As anticipated, plaintiffs and plaintiff classes have reacted to these defenses, in an attempt to find any way to recover damages for their clients who are victims of identity theft or fraud stemming from data breach. They have attempted to allege more concrete injuries, and have pleaded more causes of action, including negligence. But negligence claims are hitting a road block known as the "Economic Loss Doctrine". The doctrine has recently been applied by the Pennsylvania Court of Common Pleas in a manner that strengthens our arsenals when defending data breach lawsuits.

A Pennsylvania Precedent

In *Dittman v. UPMC***,** 2015 WL 4945713 (Pa. Com Pl. May 28, 2015), the Court of Common Pleas heard a local class action case comprised of 62,000 employees and former employees of the University of Pittsburgh Medical Center (hereinafter UPMC) whose personally identifiable information ("PII") was stolen from UPMC databases. Plaintiffs brought causes of action for negligence, as well as breach of contract. The plaintiff class claimed that UPMC breached a duty to protect their PII by failing to exercise reasonable care to protect and secure the personal and financial information. They further alleged that they incurred damages "relating to fraudulently filed tax returns[,]" and that they were at "an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse." The court dismissed plaintiffs' class action for negligence, stating that such damages amounted only to *economic loss*.

In most states, the Economic Loss Doctrine stands for the proposition that no cause of action exists for negligence that results solely in economic losses, unaccompanied by physical injury or property damage. Given that the class allegations of damages amounted solely to economic loss, with no physical injury or property damage, plaintiff class' cause of action for negligence was dismissed.

Support for the doctrine's application to data breach cases was found in the Pennsylvania Supreme Court decision in *Excavation Technologies, Inc. v. Columbia Gas Co.*, 985 A.2d 840 (Pa. 2009). This case involved allegations of negligent misrepresentation where the defendant failed to appropriately mark locations of underground gas lines. The gas lines needed to be marked around the work site, pursuant to the One Call Act. The unmarked gas lines were ultimately struck, and plaintiff suffered economic damages. Claims of negligent misrepresentation were based on defendant's failure to comply with statutory duties. A demurrer was sustained by the trial court based upon the economic loss doctrine. The Supreme Court agreed, determining that the economic loss doctrine was in existence far before the drafting of the act, and therefore, there was no statutory basis to impose liability for economic loss where the Legislature declined to do so explicitly.

The *Dittman* court followed the same reasoning in extending the economic loss doctrine to cases involving data breach. The plaintiff class argued that such a duty of care should have been imposed on UPMC to protect the confidential information of its employees. They urged the court to consider the factors set forth in *Seebold v. Prison Health Servs., Inc.* 57 A.3d 1232 (Pa. 2012) to determine imposition of a duty of care. Those The *Dittman* court followed the same reasoning in extending the economic loss doctrine to cases involving data breach. The plaintiff class argued that such a duty of care should have been imposed on UPMC to protect the confidential information of its employees. They urged the court to consider the factors set forth in *Seebold v. Prison Health Servs., Inc.* 57 A.3d 1232 (Pa. 2012) to determine imposition of a duty of care. Those factors included (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 id.* The court declined to consider these factors, stating that the Pennsylvania appellate courts had already balanced the competing interests through their adoption of the economic loss doctrine.

However, after considering these factors, the court determined that it "should not impose a new affirmative duty of care that would allow data breach actions to recover damages recognized in common law negligence actions." *Dittman* at 5. It ruled that imposing such an affirmative duty would not serve the public interest. "Data breaches are widespread. They frequently occur because of sophisticated criminal activity of third persons." *Id.* at 6. Furthermore, a private cause

*Continued on page 2*

## DATA BREACH: ECONOMIC LOSS DOCTRINE, CONT'D

of action would result in the filing of hundreds of thousands of lawsuits each year in the Commonwealth of Pennsylvania. *See id.* The court stated that "the judicial system is not equipped to handle this increased caseload of negligence actions." *Id.*

The plaintiff class arguments were complicated further by the court's recognition that there do not seem to be any generally accepted reasonable care standards in the field of data breaches. *See id.* Expert testimony and jury findings were deemed not a viable method for developing minimum requirements of care.

Public policy also weighed heavily against the plaintiff class. The *Dittman* court recognized that should a new affirmative duty be imposed, the economic impact on hundreds of corporations would be vast. This is particularly problematic where these corporations are often victims of the very same criminal activity. *See id.* at 6-7. Emphatically, the court stated "[t]he 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." *Id.* The court recognized that "[e]ntities storing confidential information already have an incentive to protect confidential information because any breach will affect their operations" and an improved system of storage would not prevent breaches in their systems. *Id.* at 7-8.

Finally, the *Dittman* court noted that the Legislature, when drafting Pennsylvania's Data Breach Act, was aware of the issues surrounding data breach cases, and only imposed a duty of notification when security systems are breached. The legislative history of this act supported the proposition that a private cause of action for data breaches was contemplated, but not created.

Other Court Support

The *Dittman* court's well-reasoned opinion was cited with approval in two subsequent federal cases from both the Eastern and Middle District of Pennsylvania; each was decided in September of 2015.

In *Enslin v. The Coca-Cola Co.*, 2015 WL 5729241 (E.D. Pa. 2015), plaintiff alleged a breach of his PII in connection with a theft of a company laptop. At the outset, it is important to note that, while establishing Article III standing in federal jurisdictions have been a large hurdle in data breach cases, the *Enslin* court determined that the plaintiff sufficiently alleged injury-in-fact. The court distinguished the Third Circuit case of *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011) as well as the Supreme Court's decision of *Clapper v. Amnesty Int'l, USA*, 113 S. Ct. 1138 (2013), and found that the injuries claimed by Plaintiff class were "ongoing, present, distinct, and palpable harms." *See Enslin*, *supra* at *6. Plaintiff had suffered theft of funds from his bank account, unauthorized use of and authorization of credit cards, and other injuries.

However, plaintiff's claims of negligence were dismissed under the Economic Loss Doctrine. In citing the *Dittman* court, the *Enslin* court found that plaintiff had failed to assert that he sustained any injury other than economic loss. The *Enslin* court also rejected plaintiff's claims that they meet the "special relationship" exception to the doctrine. This exception is found where by virtue of the respective strengths and weaknesses of the parties, one party has the power to take advantage of or exercise undue influence over the other. *See Valley Forge Convention & Visitors Bureau v. Visitor's Servs., Inc.*, 28 F. Supp. 2d 974, 952 (E.D. Pa. 1998). This special relationship does *not* apply to parties to an arms-length business contract. *See id*. Since plaintiff could not establish such a special relationship, the court dismissed his cause of action for negligence.[1]

In *Longenecker-Wells v. Benecard Services, Inc.*, 2015 WL 5576753 (M.D. Pa. 2015), the plaintiff class contained both former employees and former customers of the defendants. Defendants held PII of these individuals, and ultimately fell victim to data breaches at the hands of unknown third parties. Defendants had suffered a similar data breach in 2011, which seemed to complicate their defenses. However, similar to *Enslin*, and possibly indicative of a trend in the federal courts for data breach cases, the court found that Plaintiff class sufficiently pled "injury-in-fact". The main injury alleged was that some of the plaintiff class members suffered fraudulently filed tax returns. While this alone may have sufficed, for our purposes, the court even stated that other allegations of future injuries or harms would also satisfy Article III standing.

The *Longenecker-Wells* court then addressed the state law claims for negligence and breach of implied contract. The court found that the Economic Loss Doctrine barred the plaintiff class negligence claims, as they failed to assert any physical injury or property damage. Of note, the court stated that "[i]ndeed, in this era, where the threat of data breaches by unknown third parties is omnipresent, regardless of what preventative measures are taken, the potential disparity between the degree of a defendant's fault and the damages to be recovered could be immensely disproportionate, resulting in drastic implications for defendants named in lawsuits as well as our economic system at large." *Id*. at *6. The court also dismissed the breach of implied contract claim, citing *Dittman, supra*, in stating that defendants anticipate data breaches regardless of what measures they take to protect themselves. Therefore, since *some* measures were taken to protect the information, it was implausible to think such a defendant would ever agree to allow private causes of action against them for data breaches committed by third parties. *See Longenecker-Wells, supra.*

Exceptions: A Word of Caution

As we all know, the legal landscape of data breach changes rapidly. It is important to note that prior to the *Dittman* court's decision, the Fifth Circuit in *Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.*, 729 F.3d 421 (5th Cir. 2013), reversed the district court's dismissal of plaintiff's negligence claims pursuant to the Economic Loss Doctrine. The court, applying New Jersey law to claims of negligence stemming from a data breach of the PII of millions of credit card holders, found the "identifiable class" exception to apply. The plaintiff class consisted of "issuer banks" who incurred the costs of replacing credit cards for their consumers. The court found that an "identifiable class must be particularly foreseeable in terms of the type of persons or entities comprising the class, the certainty or predictability of their presence, the approximate numbers of those in the class, as well as the type of economic expectations disrupted." *See id.* at 424 (citations omitted). The court also noted that New Jersey declines to use the

## DATA BREACH: ECONOMIC LOSS DOCTRINE, CONT'D

Economic Loss Doctrine where a plaintiff would be left with no remedy.

Furthermore, one should take caution from the *Enslin* decision regarding the exception as to "special relationships". Particularly in the field of health care, one can imagine that arguments could be made that this exception would apply when breaches of not just PII, but sensitive personal medical information is compromised. It is important to fully examine this exception with regard to the relationship between the parties in litigation.

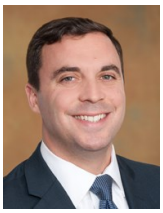
Conclusion

The Economic Loss Doctrine exists in some way, shape, or form in the majority of states. Some states narrow the doctrine to certain areas of the law, and other states provide numerous exceptions to the doctrine. Most importantly, however, is that the majority of the states which have an Economic Loss Doctrine have not been called upon to apply it to data breach litigation. This is why the *Dittman* court's decision is pivotal with regard to data breach litigation. Its reasoning as to the doctrine itself is sound, and most importantly, its opinions on the creation of a new cause of action for compromised information resulting from data breach are persuasive. While contractual claims would not be dismissed pursuant to this doctrine, the use of the doctrine adds even more ammunition for defenses to these data breach claims which at the very least, creates appealable issues and drives down costs of potential settlements.

The Cyber Security Committee of the PLDF is always willing to discuss these issues in data breach litigation. We encourage all of our members to join this committee and join the discussions regarding this rapidly developing area of law.

**Endnote**

1. The *Enslin* court also dismissed claims for, *inter alia*, negligent misrepresentation, breach of good faith and fair dealing and fraud, but found Plaintiff stated a claim for breach of contract and restitution.



**Anthony S. Cottone** is with **Burns White's Philadelphia** office. He defends individual professionals, hospitals, and long-term care facilities, and recently he expanded his expertise into cyber liability. Reach Tony at ascottone@burnswhite.com.