8/31/2015 | Articles

Respected Jurist Dismisses Massive Data Breach Class Action

In a Case of First Impression in Pennsylvania, Respected Jurist Dismisses Massive Data Breach Class Action, Finding that an Employer has no Common Law or Implied Contractual Duty to Secure Employee Data

In a case of first impression in Pennsylvania, a widely respected Allegheny County judge, the Honorable R. Stanton Wettick, Jr., dismissed a data breach class action brought against a large healthcare system, UPMC (University of Pittsburgh Medical Center), and one of its hospitals, UPMC McKeesport. The suit, *Dittman v. UPMC,* G.D. No. 14-003285 (C.C.P. Allegheny County May 28, 2015) (Wettick, J.), was filed on behalf of the 62,000 individuals employed by UPMC hospital and healthcare facilities who claimed that their personal information was compromised in a data breach perpetrated by third-party criminal activity in early 2014. In dismissing the case, Judge Wettick affirmed the application of the economic loss doctrine — which provides that there may be no recovery for economic loss in a negligence claim absent personal injury or property damage — and also rejected plaintiffs' breach of implied contract claim. Importantly, even though the court found dismissal appropriate based upon the economic loss doctrine alone, it also considered whether a new duty of care should be imposed on an employer to protect the confidential information of its employees. In doing so, the court engaged in a broad public policy analysis which on balance militated against the establishment of an underlying duty. Policy considerations included the ubiquitous nature of data breaches, the onerous burden of defending such complex litigation, the fact that the state Legislature had declined to include within its notification statute a private cause of action, and the fact that employers were as much a victim as their employees.

Data breaches have now proliferated to the point where their daily occurrence hardly warrants mention in the news media. Virtually every business, as well as even the most cyber-secure governmental entities, has become the victim of cyber-crime, with the perpetrators ranging from lone hackers to ultra-sophisticated, state-sponsored cyber-terrorists. From a damages standpoint, many whose data has been accessed or compromised never experience any misuse and, even those who do, find that their out-of-pocket loss is almost always reimbursed by their bank, credit card company, or other financial institution. While there is a significant nuisance component in having to deal with the cancellation and renewal of credit cards, bank accounts, etc., such inconvenience is not generally recognized as a cognizable injury in civil litigation.

On the federal level, data breach class actions have encountered a threshold requirement of establishing Article III standing, at least with respect to those putative members whose information has not been misused. Although there is a split of authority, over half of the federal district and circuit courts have reasoned that the mere "increased risk" of future data misuse or identity theft is too speculative and does not satisfy the constitutional "case or controversy" requirement. In a case arising from national security issues, *Clapper v. Amnesty International,* 133 S. Ct. 1138 (2013), the United States Supreme Court provided timely support for a defendant seeking dismissal due to lack of standing.

In *Clapper,* the Supreme Court considered whether certain United States residents whose sensitive international communications could have been intercepted by the United States government under the Foreign Intelligence Surveillance Act had standing to seek a declaration that the statute was unconstitutional. The plaintiffs asserted that

they could “establish injury in fact because there is an objectively reasonable likelihood that their communications will be acquired at some point in the future.” *Id.* at 1147. In dismissing plaintiffs’ claims, the Supreme Court held that the “theory of future injury is too speculative” to satisfy the “well-established” requirement of an actual injury. *Id.* at 1143. Although not a data breach case, *Clapper* highlights the inclination on the part of many courts to decline to recognize claims involving speculative future injuries, especially where such injuries are perpetrated by and dependent on the independent acts of criminal third parties. With *Clapper* providing a formidable hurdle to overcome the Article III standing requirements, data breach filings have shifted to state court venues. However, in many instances, the state courts proved even less receptive than the federal ones.

In *Dittman,* the factual predicate was favorable to plaintiffs because key financial and personal information of the 62,000 individuals employed at UPMC hospitals and healthcare facilities was accessed and compromised by third-party criminal actors. Indeed, several hundred employees had fraudulent income tax returns filed on their behalves. Plaintiffs asserted two causes of action: negligence and breach of implied contract. In a thoughtful and tightly-reasoned opinion, the trial court sustained the preliminary objections filed by UPMC and UPMC McKeesport and dismissed the case in its entirety.

In considering the negligence claim, the trial court determined that it was precluded by the judicially-created economic loss doctrine under Pennsylvania law. The doctrine provides that there may be no recovery for economic loss in a negligence action unless the individual seeking recovery has sustained personal injury or property damage. Pennsylvania courts have created an exception to the doctrine only where economic losses are sustained as the result of reliance on advice given by professionals. As there were no allegations of physical injuries or property damage and the case did not fall within the limited exception to the rule, the court held that the doctrine served to bar plaintiffs’ negligence claim in its entirety.

Notwithstanding its conclusion that the claim was barred by the economic loss doctrine, the court went on to examine whether under Pennsylvania law there was justification for the creation of a “new” duty on the part of an employer to protect the confidential information of its employees. The court explained that Pennsylvania Supreme Court case law, via *Althaus v. Cohen,* 756 A.2d 1166 (Pa. 2000), and *Seebold v Prison Health Services, Inc.,* 57 A.3d 1232 (Pa. 2012), has established a five-factor analysis for courts to consider in determining whether to impose a new duty of care. While the *Althaus/Seebold* factors need not be considered in negligence cases involving purely economic loss, Judge Wettick nonetheless considered the factors and did not find that a new affirmative duty should be created in order to permit data breach actions to recover damages in a common law negligence claim.

Engaging in a broad policy analysis, the court explained that the Pennsylvania Supreme Court had previously cautioned against imposing “affirmative new duties” unless “the change will serve the best interests of society” and “the consequences are clear.” *See Seebold, supra* at 1245. With regard to those “consequences” in this particular case, the court considered the frequency of data breaches, the potential impact of lawsuits on small businesses and non-profit corporations, and the fact that the Pennsylvania General Assembly considered but declined to adopt a provision creating a private cause of action within its notification statute, the Breach of Personal Information Notification Act, 73 P.S. § 2301, *et seq.*

In sum, the court held that businesses themselves are as much victims of the cyber-criminals as are the employees whose data is compromised. Moreover, the court pragmatically recognized that smaller businesses and non-profit corporations could be driven to financial ruin by the enormous burden of having to defend against expansive class action litigation involving thousands of individuals with no clear limiting principal on liability. Finally, the court deemed it very significant that the Pennsylvania General Assembly considered but declined to adopt a provision creating a private cause of action when it enacted the Breach of Personal Information Notification Act.

With respect to the claim for breach of implied contract, the trial court dismissed it out-of-hand. It explained that the formation of an implied contract requires a “meeting of the minds” and is not simply “an agreement imposed on parties to achieve justice.” Judge Wettick concluded that there were no facts pled which would support the “finding of an agreement between the parties under which UPMC agreed to be liable to its employees for criminal acts of third parties.” Indeed, plaintiffs had not described any exchanges between themselves and UPMC or any promises made by UPMC to plaintiffs.

Conclusion

The defining characteristics of data breaches are emerging in a way that for multiple reasons renders them entirely unsuitable for management by way of the class action process. First, data breaches have become so prolific and expansive that they affect at times tens of millions of potentially overlapping individuals. Second, the “injury” — a risk of misuse — in virtually all instances is entirely speculative. Third, out-of-pocket loss is almost always reimbursed by the bank or other financial entity. Fourth, employers are already incentivized to protect employee data and are as much a victim of the data breach as their employees. Fifth, successful attacks on the highest level of governmental entities make clear that no foolproof security measure exists.

These facts coalesce in favor of a public policy recognition by courts that each of the countless millions of “victimized” individuals cannot have a cognizable legal claim. As Judge Wettick aptly commented in the *Dittman* Opinion:

> 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.

Andrew T. Tillapaugh

John C. Conti
412-392-5425
jconti@dmclaw.com

Christopher T. Lee
412-392-5491
clee@dmclaw.com