Pepper Hamilton LLP
Attorneys at Law

CLIENT ALERT

June 12, 2015

Employees Who Suffer Only Economic Losses From a Data Breach Cannot Sustain a Negligence Claim Against Their Employer

Susan K. Lessack | lessacks@pepperlaw.com
Angelo A. Stio III | stioa@pepperlaw.com
Tracey E. Diamond | diamondt@pepperlaw.com
Brian R. Zurich | zurichb@pepperlaw.com

CREATING A PRIVATE CAUSE OF ACTION IN NEGLIGENCE FOR DATA BREACHES COULD RESULT IN THE FILING EACH YEAR OF POSSIBLY HUNDREDS OF THOUSANDS OF LAWSUITS BY PERSONS WHOSE CONFIDENTIAL INFORMATION MAY BE IN THE HANDS OF THIRD PERSONS.

On May 28, the Court of Common Pleas of Allegheny County, Pennsylvania, handed a victory to employers by dismissing a class action complaint brought on behalf of employees and former employees of the University of Pittsburgh Medical Center (UPMC). In *Dittman v. UPMC d/b/a The University of Pittsburgh Medical Center*, No. GD-14-003285 (Pa. Ct. Comm. Pl. May 28, 2015), the employees sought to recover alleged damages from the theft of confidential employment information when hackers obtained unauthorized access to UPMC's payroll system. The stolen personal data included names, birthdates, Social Security numbers, tax information, addresses, salaries and bank account information.

The class representatives asserted a claim for negligence, claiming that UPMC breached its duty of care to protect and secure its employees' personal and financial information, and also asserted a claim for breach of an implied contract, alleging that UPMC breached contract terms to protect the security of employee information it maintained. UPMC filed preliminary objections arguing, among other things, that (i) the class representatives did not have standing to maintain an action premised on a hypothetical future injury, (ii) the negligence claim was barred by the economic loss doctrine, and (iii) the breach of contract claim failed for lack of mutual intent and consideration.

The court sustained preliminary objections on both claims. Citing the Pennsylvania Supreme Court's 2009 opinion in *Excavation Technologies, Inc. v. Columbia Gas Co.*, 985 A.2d 840 (Pa. 2009), the court concluded that, under the "economic loss doctrine," no cause of action can exist for negligence that resulted solely in economic losses unaccompanied by physical injury or property damage.

The Court Finds That the Economic Loss Doctrine Applies to Bar Negligence Claims Arising from a Data Breach

The plaintiffs in *Dittman* argued that *Excavation Technologies* was not controlling and that the court should follow instead the Pennsylvania Supreme Court's prior decision in *Bilt-Rite Contractors, Inc. v. Architectural Studio*, 866 A.2d 270 (Pa. 2005), which mandated recovery for negligent misrepresentation based on an architect's liability for economic damages caused to third parties. However, as in *Excavation Technologies*, the court in *Dittman* limited the *Bilt-Rite* holding to losses that resulted from reliance on the advice of professionals in the business of supplying information for economic gain. Because UPMC is not a professional advisor, the narrow exception to the economic loss doctrine was inapplicable. Moreover, because the only damages allegedly sustained by the UPMC employees and former employees were economic losses, the negligence claim was not viable. In that circumstance, the court noted that there was no need to consider whether UPMC owed a duty of care to the class representatives.

The *Dittman* court also dismissed the claim for breach of implied contract. The class representatives alleged that, pursuant to the terms of an implied contract, they agreed to make their personal information available to UPMC, and, in exchange, UPMC agreed to safeguard and protect that personal information. The court held that no implied contract existed because there was no "meeting of the minds." The complaint contained no description of an agreement between the parties or of communications between the parties in which UPMC made any promises. As the court noted, there would be 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."

The Court Finds That UPMC Was as Much a Victim as Its Employees

In rendering its decision, the court analyzed the public policy implications of allowing a lawsuit against employers for data breaches by third parties to continue and made three significant observations. First, in dismissing the claims, the court observed that "[d]ata 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." According to the court, creating a private cause of action in negligence for data breaches "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."

Second, the court considered the substantial resources that employers would have to spend in responding to lawsuits for data breaches grounded in negligence and breach of contract. The court stated, "[t]hese 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." In this regard, the court noted, "the best interests of society would [not] 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. . . . An 'improved' system for storing confidential information will not necessarily prevent a breach of the system. These entities are also victims of criminal activity."

Finally, the court recognized that the Pennsylvania legislature already enacted legislation in the data breach arena (the Data Breach Act), which addressed the obligations of entities that suffer a breach of their security systems. In the event of a data breach, the act requires the entity to notify the individuals affected by the data breach and affords the Office of Attorney General exclusive authority to bring an action for violation of that notification requirement, but it does not contemplate a private cause of action. Because the legislature has considered the issues raised by the class representatives and has not, to date, imposed a duty of care upon entities whose security systems are breached, the court concluded that it was not appropriate for a court to create a new duty. Any further developments should be within the province of the legislature.

The *Dittman* case is not unique in its holding. The dismissal of the negligence claims based on the economic loss doctrine is supported by prior Pennsylvania decisions. In two Pennsylvania cases arising out of a data breach that occurred at BJ's Wholesale Club, for example, the courts found that the economic loss doctrine barred the plaintiffs' negligence claims because the alleged losses were solely economic in that they related primarily to the costs of issuing new credit cards to replace the ones that had been compromised by the breach.[1]

Application of the economic loss doctrine to bar a negligence claim varies from state to state, however, and other states have allowed negligence claims related to a data breach to proceed, even in the absence of physical injury or property damage.[2] For example, in a recent opinion in the Target data breach litigation, the court concluded that the economic loss doctrine did not bar the plaintiffs' Pennsylvania-based negligence claims because the plaintiffs had sufficiently alleged that Target owed them an independent fiduciary-like responsibility to safeguard their confidential information, which met Pennsylvania's "special relationship" exception to the economic loss doctrine.[3] In determining whether the economic loss doctrine will be a viable defense to a particular data breach claim, employers should investigate whether there are any applicable limits or exceptions to the economic loss doctrine under the applicable state laws.

Likewise, as we have reported previously,[4] victims of data breaches face difficulty when pursuing claims related to data breaches if there is no demonstrable injury or imminent threat of a future injury. The *Dittman* case continues the tradition in this jurisdiction of dismissing, under the economic loss doctrine, data breach–related negligence claims that involve only economic damages.

Endnotes

1. *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 427 F.Supp.2d 526 (M.D. Pa. 2006), *aff'd in part, rev'd in part on other grounds*, 533 F.3d 162 (3d Cir. 2008); *Banknorth N.A. v. BJ's Wholesale Club, Inc.*, 442 F.Supp.2d 206 (M.D. Pa. 2006).

2. *Compare In re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489, 498–99 (1st Cir. 2009) (affirming dismissal of negligence claim in a data breach case based on the economic loss rule); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F.Supp.2d 942, 967 (S.D. Cal. 2014) (same) *with Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421, 423–27 (5th Cir. 2013) (applying New Jersey law, the Fifth Circuit found that the economic loss doctrine did not bar plaintiffs' data breach claims); *Cumis Ins. Soc'y, Inc. v. Merrick Bank Corp.*, 2008 U.S. Dist. LEXIS 78451, at *19–22 (D. Ariz. Sept. 18, 2008) (denying motion to dismiss based on economic loss rule in data breach matter).

3. *In re Target Corp. Customer Data Sec. Breach Litig.*, MDL No. 14-2522, Memorandum and Order (D. Minn. Dec. 18, 2014).

4. For more information, see our previous articles: "Lack of Typicality and Adequacy of Representation Prevents Class Certification in Health Care Data Breach," available at http://www.pepperlaw.com/publications/lack-of-typicality-and-adequacy-of-representation-prevents-class-certification-in-health-care-data-breach-2015-06-08/; "Standing and the Emerging Law of Data Breach Class Actions," available at http://www.pepperlaw.com/publications/standing-and-the-emerging-law-of-data-breach-class-actions-2015-04-06/; "Federal Court Holds that Data Breach Plaintiffs Have No Standing Unless They Show Misuse," available at http://www.pepperlaw.com/publications/federal-court-holds-that-data-breach-plaintiffs-have-no-standing-unless-they-show-misuse-2015-03-24/; and "Class Actions Adding to the Cost of Data Breaches," available at http://www.pepperlaw.com/publications/class-actions-adding-to-the-cost-of-data-breaches-2012-10-24/.