Data Breach Liability for Pennsylvania Employers Expands – Pennsylvania Supreme Court Holds that Employers Have a Duty of Care to Protect and Secure Employee Data

Insights
12.28.18

Data breach liability for Pennsylvania employers of all sizes expanded with a recent Pennsylvania Supreme Court decision in Dittman v. UPMC. __ A.3d __, No. 43 WAP 2017, 2018 WL 6072199 (Pa. 2018). The Pennsylvania Supreme Court has reformed two legal principles that have protected employers against liability when they find themselves victims of third party hackers. In the wake of the Dittman decision, Pennsylvania employers – of all sizes – can no longer sit idle and should heed the opinion as a strong warning to review, assess, and revamp the adequacy (or inadequacy) of their data security protections, policies, and procedures.

Background

On June 25, 2014, Barbara Dittman along with six other employees of the University of Pittsburgh Medical Center (UPMC) filed a class action complaint asserting negligence and breach of implied contract claims against UPMC for a data breach that compromised the personal information of all 62,000 employees and former employees of UPMC. The employees alleged that a data breach had occurred through which the personal and financial information, including names, birth dates, Social Security Numbers, addresses, tax forms, and bank account information was accessed and stolen from UPMC's computer systems. UPMC had required the employees to provide the personal data as a condition of their employment. The stolen personal data was ultimately used to file fraudulent tax returns and collect tax refunds on behalf the victimized employees, resulting in actual damages.

The trial court granted UPMC's preliminary objections and dismissed the employees' claims before any discovery had occurred, finding that UPMC did not breach any cognizable legal duty and that the Pennsylvania's "economic loss doctrine" precluded the employees' claims (i.e., no cause of action exists for negligence that results purely economic losses unaccompanied by physical injury or property damage). The Superior Court sustained the dismissal and adopted the trial court's reasoning. The lower courts were explicitly concerned with the ramifications of imposing a legal duty on employers that could subject them to "hundreds of thousands of lawsuits."

The Pennsylvania Supreme Court granted allowance of appeal to address two issues:

1. Does an employer have a legal duty to use reasonable care to safeguard sensitive personal information of its employees when the employer chooses to store such information on an internet accessible computer system?

2. Does the economic loss doctrine permit recovery for purely pecuniary damages which result from the breach of an independent legal duty arising under common law, as opposed to the breach of a contractual duty?

Duty to Use Reasonable Care

The Pennsylvania Supreme Court, in reversing the lower courts, held that employers that store and collect their employees' personal data have a common law duty to protect that information. Employees argued that, in collecting and storing the sensitive personal financial information it requires employees to provide, UPMC owed a duty to the employees to exercise reasonable care under the circumstances, which includes using reasonable measures to protect the information from the foreseeable risk of a data breach. The employees alleged that UPMC's affirmative conduct created the risk of a data breach – UPMC allegedly collected and stored on its internet-accessible computer system without use of adequate security measures, including proper encryption, adequate firewalls, and an adequate authentication protocol. The Pennsylvania Supreme Court found it sufficient that UPMC required certain personal and financial information as a condition of employment, which it collected and stored on internet accessible computers. In other words, UPMC went beyond mere possession of employee information.

UPMC also argued that the third-party hacking created a superseding event that absolved UPMC of liability, relying on the general principle that the wrongful actions of a third party are not deemed foreseeable and may serve as a superseding event to prohibit liability. The Pennsylvania Supreme Court did not agree that third-party criminality eliminated the duty UPMC owed to its employees. Rather, the Pennsylvania Supreme Court noted that "liability could be found if the actor 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 a crime." Applying this principle, the Court found that UPMC created conditions that allowed cybercriminals to take advantage of the vulnerabilities in UPMC's computer systems. The Court further explained that this was not a "new affirmative duty of care"; rather, it was a mere application of an "existing duty to a novel factual scenario."

Economic Loss Doctrine

The employees' negligence claim had one additional hurdle to overcome – did the economic loss doctrine preclude their negligence claims that seek to recover purely economic damages? By way of background, the economic loss doctrine does not permit a negligence claim to proceed against a party that results solely in economic damages. The Pennsylvania Supreme Court analyzed the decisions in two Pennsylvania cases, Bilt-Rite Contractors, Inc. v. The Architectural Studio and Excavation Technologies, Inc. v. Columbia Gas Co. and concluded that these two cases do not stand for the proposition that the economic loss doctrine precludes all negligence claims seeking solely economic damages.

The Pennsylvania Supreme Court explained that the application of the economic loss doctrine "turns on the determination of the source of the duty plaintiff claims the defendant owed." The

Pennsylvania Supreme Court found that "if the duty arises under a contract between the parties, a tort action will not lie from a breach of that duty. However, if the duty arises independently of any contractual duties between the parties, then a breach of that duty may support a tort action." The economic loss doctrine did not bar the employees' negligence claim against UPMC because the Court found that the common law duty to act with reasonable care existed independently from any contractual obligations between the parties.

Employer Takeaways

The fact pattern in Dittman is certainly not a novel one. Indeed, the fact pattern is quite common and should serve as a wake-up call for employers to strengthen its data protection efforts. Data breach litigation will almost certainly be on the rise in Pennsylvania after the Dittman decision. The days of employers achieving early dismissal of data breach claims before any discovery is required are likely gone. Employers are now on notice that they have a duty of reasonable care to ensure their systems are equipped with adequate security measures to guard against data breaches.

While the steps taken by employers may vary slightly based on the employer's size or type of business, employers should follow the following general approach:

1. Consult with Human Resources professionals to review and tighten internal policies and procedures related to data protection in the area of both data collection and storage. All too often companies are collecting more data than necessary, so employers should be determining what personal information is necessary to collect in the first place. Equally important is ensuring that the information is securely stored.
2. Engage information technology personnel to develop the most effective way to adequately protect its employee data. This should happen frequently to ensure the company accounts for new data security risks that are continually developing.
3. Ensure that all of the company's employees are adequately trained in the area of data security, from the lowest level to the highest level of employees. In other words, the importance of data protection should penetrate the entire workforce and all employees should be made aware of the company's policies and procedures. It is meaningless to have policies if employees do not know about or understand the significance of violating such policies.
4. Maintain adequate documentation of the company's data protection efforts, policies, and trainings.
5. Develop a protocol for the company to follow to respond to any data breach and notify its employees consistent with the various state laws, although the company's focus should be primarily on preventing a data breach from occurring in the first place.

The bottom line is that an employer owes its employees a duty to exercise reasonable care to protect the employees against unreasonable risk of harm in collecting and storing employees' data on the employer's computer systems. Development of what "reasonable care" and "unreasonable risk" means is left to be determined, but one thing for certain is doing nothing to prevent and respond to data breaches is insufficient and could expose the company to significant legal risk.