



# Pennsylvania Employers Have a Duty to Safeguard Employees' Data, Says High Court

FEBRUARY 6, 2019 | PUBLICATIONS

Late last year, the Supreme Court of Pennsylvania ruled that employers have a legal duty to safeguard employee's sensitive personal information stored on an internet-accessible computer system and that the state's economic loss doctrine allowed the plaintiffs in *Dittman* to recover for purely monetary damages.

In 2014, Barbara Dittman and six other employees of University of Pittsburgh Medical Center (UPMC) filed a class action complaint against UPMC, alleging that a data breach occurred in which all 62,000 current and former UPMC employees' personal and financial information was accessed and stolen from UPMC's computer system. The plaintiffs further alleged that hackers used the stolen information, which included birth dates, social security numbers, tax forms, and bank account information, to file fraudulent tax returns on behalf of the employees.

The plaintiffs asserted claims of negligence and breach of implied contract against UPMC in trial court. In asserting their negligence claim, the plaintiffs claimed that UPMC had a duty to exercise reasonable care, such as using proper encryption, adequate firewalls, and authentication protocols, to protect their personal and financial information. The trial court dismissed the plaintiffs' negligence claims and rejected their arguments under PA's economic loss doctrine, and the appeals court affirmed.

On appeal to the Pennsylvania Supreme Court, a three-judge panel unanimously reversed the lower courts' ruling and held that UPMC had a legal duty to exercise reasonable care to safeguard its employees' sensitive personal information. The Court held that UPMC's affirmative act of collecting certain personal and financial information from current and potential employees created a foreseeable risk of harm, and the risk of criminal activity by a third party does not constitute an intervening act nor alleviate UPMC from its now-established legal duty. Moreover, the Court stated that it was not creating a new duty of care, but rather applying an existing duty to a novel factual scenario.

Having found that a duty exists, the Court ruled that recovery for purely pecuniary damages is allowed under Pennsylvania's economic loss doctrine, provided that a plaintiff can establish defendant's breach of a legal duty under common law that is independent of any contractual duty between the parties. Applying those conclusions to the instant case, the Court ruled in favor of the class action plaintiffs.

While the *Dittman* decision for the moment applies only in Pennsylvania, its message is clear. All employers who collect sensitive personal information from their employees must be aware of the increasing risks of doing so, not only from a practical context, but from a legal one as well. In Pennsylvania and beyond, the changing landscape of data collection practices, the increasing risk of data breaches, and the data and privacy industries in general mean that this duty to safeguard personally identifiable information may extend beyond the employment context to other industries and entities that customarily collect and store this information. Whether you would like to discuss the effect of *Dittman* on your data practices or to review your data privacy needs generally, the attorneys in the Data Privacy and Cybersecurity Practice Group are well-equipped to assist.

This post was drafted by [Tom Hayde](#), a partner in the St. Louis, MO office, and [Jay Ji](#), an associate in the St. Louis, MO office. For more information visit [spencerfane.com](http://spencerfane.com).

## AUTHORS

- [Thomas W. Hayde, CIPP/US](#)
- [Jay Ji](#)

## RELATED PRACTICES

- [Data Privacy and Cybersecurity](#)

## BLOG TOPICS

- [Privacy and Cybersecurity Solutions](#)