STRADLEY RONON

Data Breach Alert

A Publication of the Stradley Ronon
Data Breach Practice

WWW.STRADLEY.COM

DECEMBER 6, 2018

Stradley Ronon Stevens & Young, LLP
2005 Market Street
Suite 2600
Philadelphia, PA 19103-7018
215.564.8000 Telephone
215.564.8120 Facsimile
www.stradley.com

With other offices in:
Washington, D.C.
New York
New Jersey
Illinois
Delaware

Pennsylvania Supreme Court Recognizes Legal Duty to Safeguard Employee Data From Hackers

In a decision published last week, the Pennsylvania Supreme Court held that Pennsylvania employers have a legal duty to safeguard their employees' electronically stored, sensitive personal information, and failing to do so could leave the employer liable for money damages. As state, federal and international cybersecurity regulations continue to develop in response to everchanging and expanding cyber threats, the court's decision signals expanded data breach liability for Pennsylvania employers, both big and small.

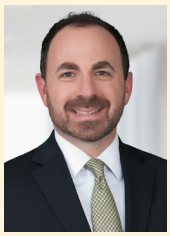
In *Dittman v. UPMC* (http://www.pacourts.us/assets/opinions/Supreme/out/Majority%20Opinion%20%20VacatedRemanded%20%20103781650446044409.pdf?cb=1), Pennsylvania's highest court confirmed the existence of a common law duty to protect employees' sensitive information. The *Dittman* plaintiffs – a class of current and former University of Pittsburgh Medical Center employees – allege that UPMC negligently exposed their sensitive personal information to hackers by failing to adopt adequate safeguards. Specifically, the employees alleged that UPMC failed to (1) properly encrypt data, (2) establish adequate firewalls or (3) implement an adequate authentication protocol – all steps reasonably necessary to protect the employees' confidential information. As a result of the breach, the plaintiffs claim they suffered economic harm and have been placed at an increased risk of identity theft. The Pennsylvania Supreme Court agreed that the employees properly presented a valid claim, and reversed previous opinions that Pennsylvania employers do not owe a duty to their employees to "exercise reasonable care in collecting and storing their personal and financial information."

The gist of the employees' data breach claim is not uncommon. In 2014, UPMC announced that hackers may have compromised the sensitive personal information of all of UPMC's more than 62,000 employees. The employees then alleged that the compromised data included Social Security numbers and bank account information as well as dates of birth, full legal names and addresses. They also alleged resulting harms including that criminals had filed false tax returns under the names of some employees, as well as employees' increased risk for identity theft and monitoring expenses.

The *Dittman* court noted that UPMC employees were required to provide personal information as a condition of their employment, which requirement the court pointed to in explaining its conclusion that UPMC had a duty of care, to protect that information from being compromised. Moreover, the court found that the failure to exercise reasonable care to protect the information constitutes actionable negligence. The court's decision reinstates the employees' lawsuit, and the case will now return to the lower court for further proceedings. If UPMC is found liable, it may be required to pay money damages to the employees.

The impact of the decision is clear: Pennsylvania now recognizes that employers owe their employees a common law duty of care to keep their sensitive personal information safe from data breaches. While the extent of this duty remains unclear, the court also found that allegations of inadequate encryption and firewalls, and lack of a proper authentication protocol (e.g., dual-factor authentication), were sufficient to articulate a claim for lack of due care. Steps for

Pennsylvania employers to take now include: (a) consult with information technology personnel to determine whether employee data is adequately protected with data encryption, firewall and authentication protocols; (b) consult with human resources personnel to review employee data collection and storage processes to confirm that only necessary employee private information is collected, and that such information is securely stored; (c) develop protocols for immediate response to cybersecurity incidents; (d) train or re-train employees regarding maintaining data security; and (e) communicate with the company's insurance broker regarding existing or available insurances, including but not limited to cyber insurance, to cover the company in the event of a liability arising from a data breach or hacking incident.



Jeffrey D. Grossman

Kristin J. Jones, CIPP/US

Mischa S. Wheat

For more information, contact Jeffrey D. Grossman at 215.564.8061 or jgrossman@stradley.com, Kristin J. Jones at 484.322.1335 or kjones@stradley.com, or Mischa S. Wheat at 215.564.8597 or mwheat@stradley.com.