Client Alert: Pennsylvania Supreme Court Requires Employers to Protect Employee Information from Computer Hacks

Related Professionals

Andrew C. Smith

Michael C. Griffaton

Related Services

Data Strategy, Privacy and Security

Labor and Employment

Litigation and Appeals

CLIENT ALERT | 11.30.2018

On November 21, 2018, the Pennsylvania Supreme Court issued a far-reaching decision that "an employer has a legal duty to exercise reasonable care to safeguard its employees' sensitive personal information stored by the employer on an internet-accessible computer system." Employers in Pennsylvania now have a common law duty to protect their employees' information from potential data breaches.

In *Dittman v. University of Pittsburgh Medical Center* (UPMC), employees alleged that a 2014 data breach at UPMC had exposed the personal and financial information of 62,000 employees and former employees, including names, birth dates, Social Security numbers, addresses, tax forms, and bank account information. The employees claimed that they had been required to provide UPMC with this information during their employment. As a result of the breach, the employees claimed they were the victims of fraudulent tax returns and remained at risk for future identity theft. In essence, negligence claims argue that a defendant had a duty to take some action but failed to do so. Here, UPMC's employees argued that, because UPMC required them to provide sensitive information in order to be employed, it had a common law duty to protect that information from theft or unauthorized disclosure. The class action alleged UPMC was negligent in how it maintained and protected the sensitive information that UPMC collected from its employees.

Both the trial court and appeals court dismissed the claims, finding that Pennsylvania law precluded negligence claims where no physical injury or property damage occurred. The trial court voiced concerns about data breaches becoming more frequent, stating that if negligence claim were allowed in these situations, "hundreds of thousands of lawsuits" would follow, overwhelming courts with cases and employers with unreasonable costs. The appeals court stated that "[e]mployers strive to run their businesses efficiently and they have incentive to protect employee information and prevent these types of occurrences," and so negligence claims were not needed to incentivize employers to protect sensitive employee information.

The Pennsylvania Supreme Court rejected the lower courts' reasoning, which sets the case for trial. The Supreme Court held that employers who collect and store sensitive information could be found negligent if that information is stolen. The Court rejected UPMC's arguments that it was not liable because of the illegal activity committed by those who breached UPMC's computer systems and stole the information. Instead, the Court held that, by "collecting and storing the Employees' data on its computer systems," UPMC itself created the risk of a data breach in the first place, and thus it owed a duty to its employees to take reasonable steps to protect that information.

The Court did not say what specific steps employers must take to meet their duty. Nonetheless, the Court held that where an employer fails to use security measures such as "encrypting data properly, establishing adequate firewalls, and implementing adequate authentication protocol," the employer could be liable if the data is stolen. The Court compared weak data security to a building owner whose dilapidated building starts a fire because it was not safely maintained.

In light of the Pennsylvania Supreme Court's decision, employers should review their data collection and storage policies and procedures. If your company collects Pennsylvania employee records that contain sensitive personal information, contact your Vorys attorney to discuss how to limit the company's potential liability.