CARLTON FIELDS

Building an Ark: Protecting Employee Data in the Data-Breach Era

April 04, 2019

Recent years have seen not so much a leak as a flood of data breaches affecting companies nationwide. But the traditional systems devised to safeguard against data breaches won't withstand the vulnerabilities created when information is shared with third-party providers. And although companies are somewhat buoyed by legislation to protect against cyberattacks, companies are often left adrift in a sea of uncertainty as the wave of cybersecurity risks threatens to rise.

As risk levels rise, however, so too does an employer's responsibility to re-evaluate its data security practices. On November 21, 2018, in *Dittman v. UPMC*, the Pennsylvania Supreme Court held that employers have a common-law duty to protect their employees' sensitive personal information stored on an internet-accessible computer.

In *Dittman*, a group of employees filed a class action lawsuit against their employer after a data breach resulted in the theft of sensitive personal information of thousands of employees. The stolen information, which the employees were required to provide as a condition of employment, was stored on the employer's computer systems and ultimately used to file fraudulent tax returns, resulting in damages to the employees. The employees asserted claims of negligence and breach of implied contract, alleging that the employer failed to maintain adequate security measures — including in accordance with industry standards on cybersecurity — to safeguard employees' information.

The trial court dismissed the case, holding that the economic-loss doctrine, as decided in prior appellate rulings, precluded the employees' claims, which asserted solely economic losses. The trial court also declined to impose a new affirmative duty of care to protect data, noting that the financial impact of doing so could put entities out of business. On appeal, the Superior Court upheld the dismissal and held that the trial court properly determined that the employer owed no duty to its employees under Pennsylvania law.

The Pennsylvania Supreme Court reversed the lower courts' decisions, applying an existing duty of care to a novel factual scenario, and held that the employer's affirmative conduct in requiring its employees to provide personal information as a condition of employment gave rise to a duty to exercise reasonable care to safeguard that information. The duty of reasonable care includes a duty to implement reasonable security measures to protect against the foreseeable risk of a data breach, especially considering that an employer's inadequate data collection and storage practices evidently create the risk of a data breach.

Dittman has been touted as a warning to employers — but the decision has ramifications beyond those with an employer-employee relationship. Any service provider hosting or handling employee data should take heed. Therefore, it has become even more imperative that employers address the vulnerabilities created by information sharing with third-party product and service providers. And especially in industries where there is no established regulatory framework outlining specific requirements, *Dittman* is clear: build a better boat.

Related Practices

Cybersecurity and Privacy
Labor & Employment
Life, Annuity, and Retirement Litigation