PENNSYLVANIA HIGH COURT HOLDS EMPLOYERS HAVE AN AFFIRMATIVE DUTY TO PROTECT EMPLOYEES' PERSONAL DATA

Cybersecurity & Privacy Alert
November 28, 2018

The Hodgson Russ Cybersecurity & Privacy Practice has been predicting that courts would over time begin to require holders of personal information to use commercially reasonable efforts to protect the information from loss and unauthorized access, disclosure, modification and use. We have, for better or worse, again been proven correct.

The Supreme Court in Pennsylvania has now ruled that ***employers*** have an affirmative legal duty to protect their employees' personal data. This decision will cause further disruption in an already unsettled area of risk for many companies.

In February 2014, the University of Pittsburgh Medical Center ("UPMC") notified the public of a data breach. In its initial notice to the public, UPMC stated that only 22 employees were affected. In April 2014, UPMC confirmed that information stolen affected up to 27,000 employees and by May 2014, it confirmed that all current and former employees of the medical center were affected. The personal information stolen included names, birth dates, social security numbers, tax information, addresses, salaries, and bank information of former and current employees.

As the Medical Center investigated, seven current and former employees, in February 2014, brought a class action suit (representing a class of 62,000 current and former employees) against UPMC alleging negligence and breach of implied contract. In substance, the class alleged that UPMC acted negligently by failing to adopt, implement and maintain adequate security measures, such as firewalls, data encryption and authentication protocols, and by failing to monitor the security of its network. The Court of Common Pleas, Allegheny County, dismissed both counts in the complaint. First, the Court dismissed the negligence claim, as being barred by the economic loss doctrine. Second, the Court dismissed the breach of contract claim because plaintiffs' factual allegations did not sufficiently plead a meeting of the minds, as required to plead an implied contract claim. The Superior Court affirmed this decision. But, the Supreme Court reversed the lower court decisions related to plaintiffs' negligence claim, holding that the lower court's ignored an exception to the Economic Loss Doctrine that permits a negligence claim where a separate legal duty exists. Here, the Court found that UPMC owed a legal duty to its employees "to

Attorneys

Gary Schober

Practices & Industries

Cybersecurity & Privacy

exercise reasonable care in collecting and storing [employees'] personal and financial information" based, in part, on UPMC's requiring employees to provide their personal information as a condition of employment. *See Dittman v. UPMC*, 2018 WL6072199, at *9 (Pa. Sup. Ct. Nov. 21, 2018).

In its holding, the Supreme Court vacated the judgment of the Superior Court, reversed the order of the trial court and remanded the matter to the trial court for further proceedings. *Id.* at *15. It is now up to the trial court to determine whether UPMC breached its duty to employees, and whether it used reasonable care in its data protection efforts.

While this result was predicted by us, it is nonetheless a significant development in breach liability case law, and something that all employers should be cognizant of when developing their data security strategy for the protection of employees' personal information. There is also another lesson here for all of us, even those of us who do not hold employee information.

Many of the current U.S. laws that specifically require the protection of personal data apply only in certain circumstances (e.g. health care or banking). However, whether or not directly applicable to a particular set of circumstances, we must never forget that these laws establish a standard of reasonableness for protecting information. If a medical provider needs to implement reasonable measures to protect personal data, why shouldn't an employer? Indeed, why shouldn't everyone be required to use these measures? There should be no doubt that ***all*** holders of personal information will ultimately be required to implement reasonable security measures to protect personal information. *See e.g.* the California Consumer Privacy Act, which takes effect in 2020 and requires that all personal data relating to Californians must be protected using reasonable measures. To be sure, the failure to do so protect personal data could expose a business to significant liability.