CONNER & WINTERS

EMPLOYMENT LAW ALERT

IF HACKERS TARGET YOUR BUSINESS, WILL YOU BE LIABLE TO THE EMPLOYEES WHOSE DATA WAS STOLEN?

March 9, 2017

Visit us online at cwlaw.com

The question seems to no longer be whether your company will be the victim of a data breach, but when. When employers collect and store their employees' personal information, they became potential targets for hackers. If hackers steal sensitive employee data, employees may be tempted to sue for any damages caused by the hackers' use or disclosure of that information. Courts are only beginning to address the potential liability of employers in this situation and have reached differing conclusions.

Employees victimized by data breaches may seek redress from their employers on legal theories of breach of an implied contract or negligence. Implied contract claims are not likely to succeed, because employees would need to prove a difficult proposition: that their employer intended to enter a contract to protect the employees' information. Recent cases have focused primarily on negligence claims, and the success of those claims turns on whether employers have a legal duty to protect the information.

To recover under a negligence theory, an employee must demonstrate the employer had a duty to the employee, that it breached that duty, and that the breach caused damage to the employee. In a recent Pennsylvania case, *Dittman v. University of Pittsburgh Medical Center*, the court held that the University had no legal duty to its employees. Hackers had obtained the names, social security numbers, tax and banking information, birth dates, and addresses of nearly 62,000 current and former employees. With this information, the hackers filed fraudulent tax returns and stole refunds. Since the University required employees to provide this information as a condition of employment, the employees argued it owed a legal duty to protect and secure their information. The court disagreed.

Before imposing common law duties on employers, courts consider numerous factors. These factors include the relationship between the parties, the social utility of the conduct, the foreseeability of harm, the consequences of imposing the duty, the public interest in the solution, and whether creating a duty is the role of the legislature rather than the courts.

Our Labor and Employment Group Attorneys

P. Bradley Bendure
Vicki Bronson
Teresa Meinders Burkett
Kathryn S. Burnett
David R. Cordell
Isaac Ellis
John W. Funk
P. Scott Hathaway
Tony W. Haynie
Crystal A. Johnson
Kerri E. Kobbeman
Donn C. Meindertsma
J. Ronald Petrikin
Ryan T. Scharnell
Hayley N. Stephens
Jason S. Taylor
Nancy E. Vaughn
G. Alan Wooten

more ...

In *Dittman,* the court found that the employer-employee relationship weighed in favor of imposing a duty on employers to protect employee data, but that all other factors favored the University. There is obvious social utility in an employer's collection of personal information. While damage from a breach is foreseeable, the criminal act of a third party, here the cybercriminals, is typically considered a superseding event that an employer need not guard against unless it "realized, or should have realized, the likelihood of such situation."

The *Dittman* court reasoned that imposing a duty to protect employee data from hacking would not further incentivize employers to protect data. It noted that data breaches are widespread and "there is not a safe harbor for entities storing confidential information." Imposing a duty would require employers to incur significant security costs "where there is no true way to prevent data breaches altogether." The significant cost increases were not justified where employers already have incentives to protect confidential information.

" With the law on this topic in flux, employers should take reasonable steps to protect their employees' data from hackers."

Courts have also refused to impose a duty on employers out of deference to legislatures. In most states, legislatures have passed statutes that define what companies must do in the event of data theft, which is usually to notify those affected by the breach. Most of those laws do not include a duty to protect data from disclosure. The courts reason that, if the legislature wanted to impose a duty to protect the information, it would have included it in the statute.

In the California case of *Castillo v. Seagate Technologies*, however, the court found the employer had a duty to its employees to protect against the theft of personal information. In fact, the court extended this duty to the spouses and dependants of Seagate employees whose information was compromised. *Castillo* did not discuss as thoroughly as *Dittman* whether a duty should be imposed in the first place, because Seagate did not contest that it owed a duty to protect its employees' personal information. In fact, the court found that Seagate had no good reason even to argue against a duty, noting that the employees provided their information to the company as a condition of employment "with the understanding their employer would guard that information."

With the law on this topic in flux, employers should take reasonable steps to protect their employees' data from hackers. Any threats should be treated seriously. Data breach policies should be implemented and account for the possibility that employee data may be stolen. If employers discover they are victims of a data breach, they should contact counsel to develop a course of action, including assuring compliance with any breach notification laws enacted in their states. Additional steps can also be promptly taken to mitigate damage to employees and to reduce the likelihood that they will sue.

Please let us know if you have any questions about this development.