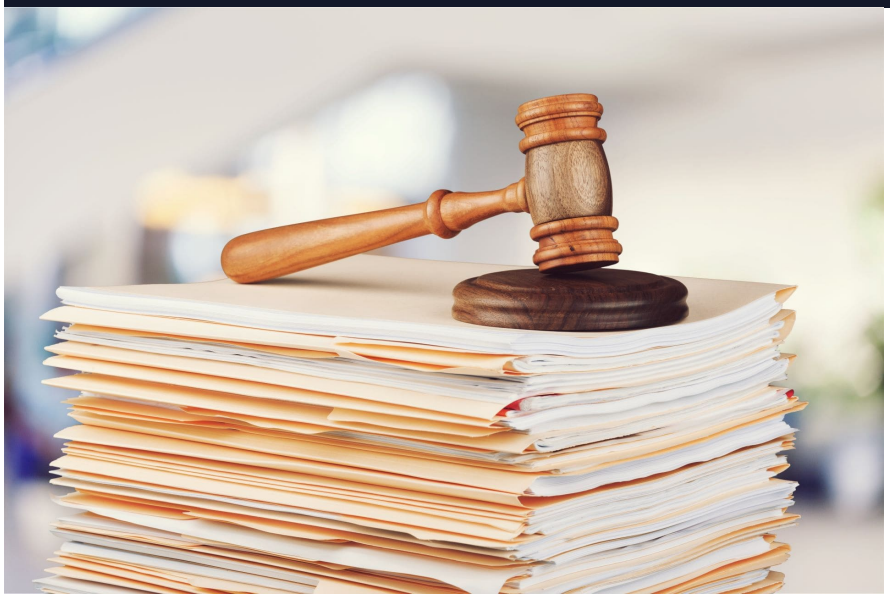
BARNES & THORNBURG LLP



ALERTS

Pennsylvania's High Court Rules On Employers' Duty Of Care In Data Breaches: What You Need To Know

January 9, 2019 | Atlanta | Chicago | Columbus | Dallas | Delaware | Elkhart | Fort Wayne | Grand Rapids | Indianapolis | Los Angeles | Minneapolis | New York | San Diego | South Bend | Washington, D.C.

If your company has operations or employees residing in Pennsylvania, you need to know about the most recent duty of care case in the data security context. Because of this case, employees in Pennsylvania may now sue their employer for economic loss resulting from the employer failing to protect the employees' sensitive information.

Why you want to know about this case

Until now, employers have not been held liable to employees for a data breach or required to pay damages suffered by the employees due to the breach. In November 2018, however, the Pennsylvania Supreme Court[1] overturned the lower court and ruled that an employer must exercise reasonable care to safeguard its employees' sensitive information stored on its computer system. And, employees may recover monetary damages for a breach of this duty if they suffer actual damages or are placed at imminent risk for future harm, such as identity theft and fraud. In this case, as a condition of employment, the employer had required employees to provide information such as birth dates, social security numbers, and financial information. A hacker accessed sensitive employee information, including tax forms, bank accounts, and other identifying information of all 62,000 current and former employees. The information was later used by the hacker to file fraudulent tax returns and obtain tax refunds.

The court reasoned that because the employer – as a condition of

RELATED PEOPLE

Jason A. Bernstein
Partner
Atlanta

P 404-264-4040
F 404-264-4033
jason.bernstein@btlaw.com

Brian J. McGinnis
Partner
Indianapolis

P 317-231-6437
F 317-231-7433
brian.mcginnis@btlaw.com

Juanita DeLoach, Ph.D.
Partner
Dallas

P 214-258-4152
F 214-258-4199
juanita.deloach@btlaw.com

RELATED PRACTICE AREAS

Data Security and Privacy

employment – required the personal information, the employer had a duty to provide adequate security measures to protect the employees' sensitive information, such as setting up adequate firewalls, providing proper data encryption, and implementing an adequate authentication protocol. The court determined that the employer failed to take such reasonable security measures and viewed that as affirmative conduct creating the risk that led to the breach and loss.

The court was not persuaded by the employer's arguments that (a) allowing recovery in this case would cause thousands of lawsuits and overwhelm the judicial system, (b) the hacking created a superseding event releasing the liability of the employer, or (c) the employer was not in the "business of providing data security."

What employers can do to reduce data breach risk and liability

We believe other states may also move in the direction of creating similar employer liability; therefore, this Pennsylvania Supreme Court decision should prompt employers operating in Pennsylvania or collecting data of employees residing in Pennsylvania to evaluate their existing cybersecurity security measures and policies.

Employers should consider implementing the following best practices:

- Make sure that employee files are stored in segregated areas on company servers and are accessible only to HR and finance personnel with proper authorization.
- Use a separate password to access employee files so that if a hacker gets access to the company's systems, employee files cannot be accessed without a second password.
- Increase the frequency of training for all employees, but particularly HR and finance personnel to improve awareness of phishing and spoofing attacks, which are among the most successful attacks suffered by companies (e.g., W-2 file theft, wire transfer fraud, etc.).
- Review any insurance program to determine whether losses resulting from a breach or disclosure of employee data (not just data of customers, patients, etc.) would be covered. Cyber insurance policies are not uniform and many contain exclusions you may not expect.

Members of Barnes & Thornburg's Data Security and Privacy group provide a wide range of services to help clients evaluate and reduce security and privacy risks, and guide clients in the event of a data breach. Our team also reviews and provides guidance on cyber insurance policies and coverage for data privacy and cybersecurity risks.

For more information, please contact the Barnes & Thornburg attorney with whom you work or Jason Bernstein at (404)264-4040 or jason.bernstein@btlaw.com, Brian McGinnis at (317)231-6437 or brian.mcginnis@btlaw.com, or Juanita DeLoach at (214) 258-4152 or juanita.deloach@btlaw.com.

---

[1]*Dittman v. UPMC, 2018 WL 6072199 (Pa. Nov. 21, 2018).*