Pennsylvania Supreme Court Ruling Opens Up Businesses To Liability For Data Breaches

Client Advisories

12.12.2018

In a recent landmark decision, the Pennsylvania Supreme Court ruled that an employer has a duty to take reasonable measures to safeguard sensitive personal information that it collects from its employees, and that the failure to fulfill this duty exposes the employer to potential liability for monetary damages. Dittman v. UPMC, --A.3d--, 2018 WL 6072199 (2018). The employer, the University of Pittsburgh Medical Center, suffered a data breach, resulting in the theft of its employees' names, birth dates, social security numbers, addresses, tax forms, and bank account information. Among other things, the employees alleged that the stolen information was used to file fraudulent tax returns, which resulted in actual monetary damages.

This decision will have wide-ranging consequences for businesses operating in Pennsylvania, whether located there or elsewhere. It will very likely apply to any sensitive personal information or health-related information that a business stores or controls, regardless of whether it is collected from or about its employees. Furthermore, there are similar and persistent movements by other states and the federal government to extend a business's obligations to prevent hackers and other criminals from unauthorized access to personal information.

In Dittman, the employees claimed that UPMC failed to use "proper encryption, adequate firewalls, and an adequate authentication protocol." Other businesses may consider different or more or less stringent measures, depending upon their circumstances. At the very least, any business that does little or nothing to protect sensitive personal information against unauthorized access runs a substantial risk of liability if Pennsylvania law or other laws requiring reasonable measures apply-and there are simple, minimal-cost cybersecurity measures that any business can take in nearly all circumstances.

Businesses everywhere would be wise to assess their data security policies and procedures, recognizing this growing duty to take reasonable steps to safeguard the sensitive personal information that they collect or control. A bit of proactivity now is far preferable (and much less costly) than waiting to suffer a data breach,

defending a lawsuit and being open to the potential of a large judgment or a government investigation, not to mention incurring the costs of responding to a breach.

Businesses should therefore consult with experienced legal counsel to determine their individualized needs. Various actions that a business might consider are outlined in the document titled Cybersecurity Checklist: 10 Steps To Protect Your Business that can be accessed at the following link https://archerlaw.wpengine.com/wp-content/uploads/2018/12/Client-Advisory-Cybersecurity-Checklist-10-Steps-to-Protect-Your-Buisness.pdf.

Archer's Data Privacy and Cybersecurity Group has a team of attorneys who keep abreast of developments in this quickly evolving area of the law and understand how these developments affect our clients. We provide consulting services that can be scaled according to your individual circumstances, needs and budget. We also work with technical computer experts in cybersecurity, bankers and experienced cyber insurance brokers.

If we can assist you in any way, please contact any Archer attorney with whom you are familiar, or Data Privacy and Cybersecurity Group members Robert T. Egan, Esquire at regan@archerlaw.com or 856-354-3079, Kate A. Sherlock, Esquire at ksherlock@archerlaw.com or 856-673-3919, or Daniel J. DeFiglio, Esquire at ddefiglio@archerlaw.com or 856- 616-2611.

DISCLAIMER: This client advisory is for general information purposes only. It does not constitute legal advice, and may not be used and relied upon as a substitute for legal advice regarding a specific legal issue or problem. Advice should be obtained from a qualified attorney licensed to practice in the jurisdiction where that advice is sought.

Related People

Daniel DeFiglio

Partner

ddefiglio@archerlaw.com

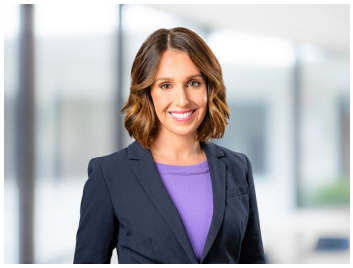
856.616.2611

Robert T. Egan

Of Counsel

regan@archerlaw.com

856.354.3079



Kate A. Sherlock

Partner

ksherlock@archerlaw.com

856.673.3919

Related Services

- Data Privacy & Cybersecurity