New Court Ruling: Employers Must Protect Employees' Identities, Personal Data

Guarding your company's most valuable asset — your employees

By Ammon Curtis

The writing is more than on the wall. It's scrawled everywhere you look, and it's in bright, flashing letters that can't be ignored. It screams at you, at everyone that passes, a single and undeniable truth: ***Businesses must protect their employees.***

This is neither a new concept nor a revolutionary idea. It is a belief many of us hold to be self-evident. And now, it is written into law.

Let's take a closer look at what a recent Pennsylvania Supreme Court (PSC) ruling means for Pennsylvania businesses, their employees, and the entire nation. But first, some context.

A Brief History of the UPMC Data Breach

Back in 2014, the University of Pittsburgh Medical Center (UPMC) experienced an unprecedented data breach: Hackers stole the personal information of more than 60,000 former and current employees.

Cybercriminals used victims' names, Social Security numbers, addresses, banking information, and other sensitive data to file fraudulent tax returns. The thieves were then able to collect the victims' tax refunds — a trend that has been growing significantly in recent years.

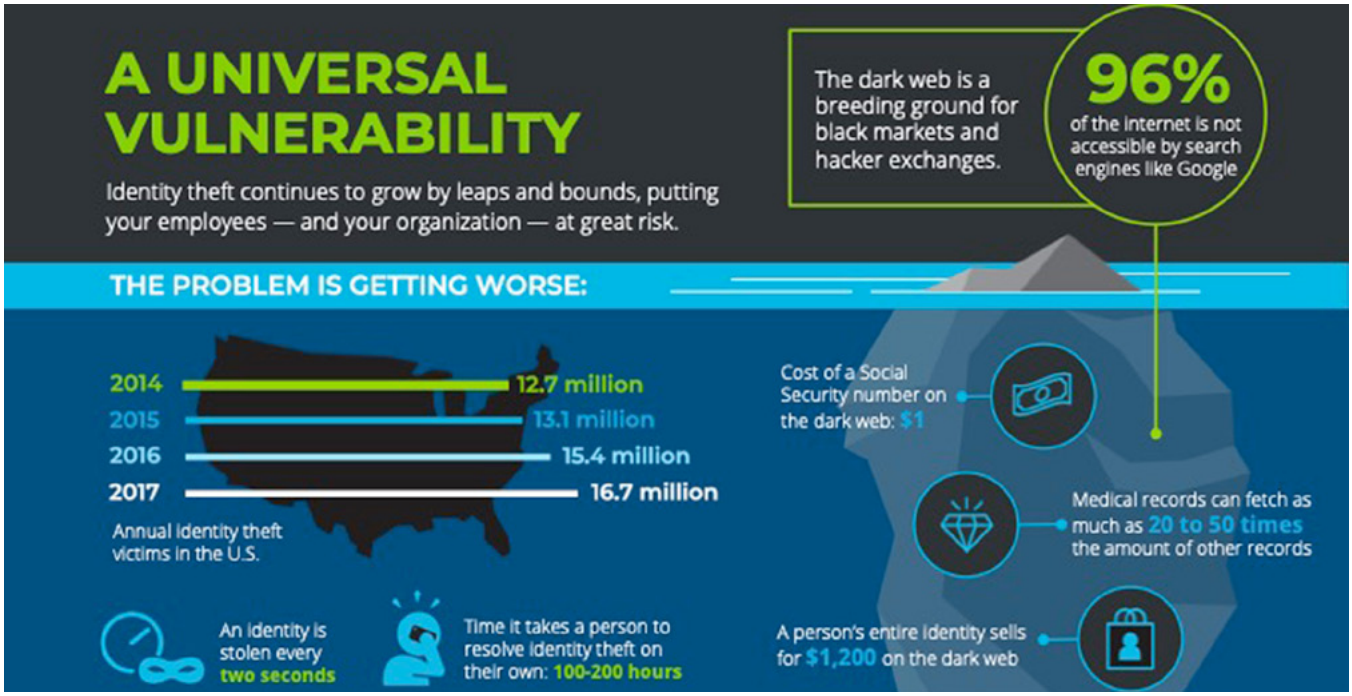
Affected employees brought a class action lawsuit against the medical center. Victims felt that, since they were required to exchange this sensitive information for employment consideration, UPMC had a responsibility to protect that data.

After a series of trials and appeals, the case reached the Pennsylvania Supreme Court. And, on November 21, 2018, the highest court in Pennsylvania sided with the aggrieved employees.

The Landmark Decision of *Dittman v. UPMC*

There were many notable elements of PSC's ruling, but the most significant is the logic the court used to reach their decision and the far-reaching implications this will likely have.

The Pennsylvania Supreme Court found that UPMC's practice of collecting and storing sensitive employee data constituted as affirmative conduct. As such, the company had a responsibility to protect all sensitive data and provide adequate security measures.



Because UPMC failed to do this, the court concluded that the data breach was "within the scope of the risk [UPMC] created."

The PSC further protected employees' right to sue negligent employers. According to the court, employees can take legal action against a company even if their employer didn't explicitly promise to protect the data it collects. A contract is not needed, as this responsibility is the employer's "common law duty."

What This Means for the Rest of Us

Dittman v. UPMC is about much more than an isolated data breach. It is bigger than one medical center's failure to protect its employees. It's even bigger than the 62,000 employees who had their data compromised.

Instead, it is about one simple truth: **Businesses must protect their employees.**

We didn't need a court to tell us this. But, now that they have, you can expect a lot more to follow suit. *Long before PSC's ruling, the legal system had been increasingly holding employers responsible for employee data breaches and identity theft.*

This isn't a bad thing. It is a necessity — one that stems from the numerous challenges posed in today's Digital Era. Helping companies meet these challenges is the whole reason we started InfoArmor, the leader in identity protection and advanced threat intelligence for more than 10 years.

We believe that everyone deserves peace of mind, and it is this belief that powers everything we do. It's why we're committed to protecting the places people work, the relationships they build, and the data they share.

If you'd like to learn more about how we do this, please schedule a demo of our award-winning employee identity protection benefit, PrivacyArmor. We'd love to help you protect your company's most valuable asset — your employees.

• • •

Ammon Curtis is the Senior Vice President of Product at InfoArmor.

Would you like to comment?

Submit Your Articles

The most extensive **employee identity protection** plan available

Attract top talent and protect your employees with **PrivacyArmor®**

Employees want it, employers need it

Our monitoring capabilities exceed those of any other provider, and we protect all types of businesses and industries without exception. PrivacyArmor scours the dark web for compromised credentials, monitors financial transactions, and alerts participants to signs of fraud that other providers don't detect. Our full restoration services help participants detect and recover from identity theft quickly so they can focus on their job.

- ✓ Seamless integration with 140+ platforms
- ✓ 99% client satisfaction rate
- ✓ 2,100+ successful client implementations
- ✓ Dedicated account manager for all your needs
- ✓ Safeguards employee productivity and well-being
- ✓ The most extensive identity protection features
- ✓ In-house 24/7 Privacy Advocate remediation and restoration
- ✓ $1 million identity theft insurance policy†

Want to learn more?

Call us at **800.789.2720** to schedule your demo of PrivacyArmor.

PrivacyArmor by InfoArmor

†Identity theft insurance underwritten by American Bankers Insurance Company of Florida. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies describe. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.