Facebook Might Pay A Fine, But Is Your Company Paying The Price?

Taking the proactive approach to protecting employee data

By Ammon Curtis

After enduring a decade of criticism from both users and regulators, it appears Facebook's privacy issues are now front and center. The organization is facing a fine from the FTC that could hit as high as $5 billion.

But as Facebook sets aside billions of dollars to begin covering the fine, who is really paying the price of privacy violations? Is it the multitudes of users whose private information was hacked, borrowed, or stolen? Or is it the companies like yours who employ them that end up paying the heaviest costs?

Facebook in the Workplace

Let's face it. Your employees are not just using Facebook at home and on their lunch breaks. They're "liking" Aunt Judy's cat pictures while writing corporate reports, working a sales floor, or sitting in meetings. It might be disturbing to admit, but in some cases, Facebook might know what employees are up to from 9 to 5 better than you do.

Although the constant distraction of social media is in itself a huge drain on productivity, it's what happens when those accounts are compromised that keeps us, as employers, up at night.

Some accounts are created with corporate emails. And many users carry identical passwords across multiple accounts. So sharing a user's private information, such as login credentials, with a partner could grant access to unrelated corporate emails, employee benefits, payroll, purchasing, or anything else that individual has access to. Even if the passwords aren't *exactly* the same, many users create them from combinations of family names, pets, initials, and birthdates. Guess what? A hacker could easily collect ALL that information from the average user's Facebook account.

Implications of Facebook Breaches

Due to the way Facebook accounts intermingle private, public, and professional information, a breach of one employee's Facebook account could:

- Expose coworkers' accounts, opening them up to another wave of identity thefts
- Exponentially expand the potential for security breaches of your own systems with each coworker compromised
- Provide threat channels into client and partner accounts, which could lead to loss of trust and even financial liabilities

Submit Your Articles

So, why is Facebook, in particular, such a concern? In addition to being a target for hackers, Facebook has dealt with privacy issues over the years. Recent events include:

- The infamous Cambridge Analytica scandal, where the political consulting firm collected personal information from millions of users via Facebook "quizzes" and exploited a loophole to gather personal data from their friends, too
- A New York Times investigation found Facebook shared user data with other technology partners without the consent of many of its subscribers
- In 2018, Facebook announced a security breach involving over 50 million user accounts

It's easy to see why this could be a concern for employers everywhere, and why many are looking at identity theft protection benefits to help reduce their risk while the U.S. and other governments tackle the issue of regulating social media.

Image Credit: *InfoArmor*

Is a Facebook fine the first step towards tighter regulations on data privacy?

The United States has *already* taken the first few steps in that direction. Levying a multi-billion dollar fine against Facebook may give those measures teeth — and let businesses know that regulators are serious about privacy protection.

Meanwhile, U.S. state courts are seeing cases involving the theft of employee data. The precedents they set could have long-term effects on how businesses view employee benefits such as identity theft protection in the future.

In a recent landmark decision, *Dittman vs. UPMC*, the Pennsylvania Supreme Court ruled that because the University of Pittsburgh Medical Center (UPMC) collected and stored sensitive employee data, it had an obligation to provide adequate security measures to keep that data safe. Because it did not, when a subsequent hack compromised the data of 62,000 employees, the court found UPMC responsible.

The implications here are highly significant for every business in the U.S. Not only did *Dittman vs. UPMC* establish the obligation of employers to provide adequate privacy protection measures for their employee's data, but it also confirmed an employee's right to sue their employer for failing to do so.

Taking the Proactive Approach to Protecting Employee Data

Making sure your workforce has privacy and identity protection is both feasible and cost-efficient. You can't afford to trust social media companies such as Facebook to have your employees' best interests in mind. The stakes are simply too high. You need to protect yourself by protecting them.

While Facebook might pay a hefty fine for its user privacy issues — and while some of those compromised users might even work for you — your company isn't getting any of it. But you'll still deal with all the normal costs of identity theft, and you'll still be on the hook in U.S. courts if they decide you failed to provide adequate protection.

So, why wait for more regulations? Make identity theft protection a keystone of your employee benefit programs… not because you have to, but because it makes good business sense to do so.

• • •

Ammon Curtis is the Executive Vice President of Product, Marketing, and Design at InfoArmor.

Would you like to comment?

Submit Your Articles

InfoArmor

Not every **superhero** wears a cape.

Defend your organization with PrivacyArmor®, the most advanced identity theft protection available.

In-house **24/7** resolution

Seamless integration with **140+ platforms**

99% client satisfaction rate

Voluntary & sponsored programs, available through benefits brokers

Learn more

© InfoArmor, Inc. All rights reserved