InfoArmor

Why Companies Should Care When Employees Have Their Identities Stolen

EBOOK

www.infoarmor.com

Intro

Year after year, identity theft is on the rise, and consumers aren't the only ones who have to pay a price. When your employee has their identity stolen, this can spell big problems for your business. Let's take a closer look at why this is the case, and, most importantly, what you can do to protect your company's greatest asset — your employees.

State of Identity Theft

With data breaches occurring at an alarming rate, it's no surprise your employees are concerned with having their identity stolen. And, given the fact that 143 million Americans -- over 80% of working adults -- had their personal data stolen from Equifax, the chance your employees will experience identity theft in the future is a very real possibility.

- Identity theft has ranked in the top three FTC consumer complaints for **17 years straight**
- Americans rate criminal hacking as the number one threat to their **health, safety, and prosperity**
- **40%** of Americans have either been the victim of identity theft or know someone who has
- **$16** billion was stolen from 15.4 million U.S. consumers in 2016
- From 2013 to 2015, ID Theft complaints increased **47%**

Employers Often Play a Role in Employee Identity Theft

One of the many reasons employers should care about identity theft is that, despite the best of efforts, they often directly contribute to their employee's identity being stolen. In fact, they are often the biggest culprit in breaching individual privacy. This is largely because state and federal laws require employers to maintain a tremendous amount of personal information on every employee, from social security numbers to addresses and more.

- Cybercriminals are able to steal the personal data of **every employee i**n one attack
- **33%** of phishing attacks come from emails designed to appear as if they are coming directly from the CEO of an organization
- **Identity theft** is often perpetrated by fellow employees and sometimes even managers and executives
- **$16 billion** was stolen from **15.4 million** U.S. consumers in 2016
- Around **30% - 50%** of all identity theft originates in the workplace

Costs to the Company

In addition to the moral obligation an employer has to help protect their employees' identities, they also have a financial one. When employees have their identities stolen, companies pay big.

- Courts are increasingly holding employers liable for the **loss of their employees'** confidential information, even in the absence of a specific law requiring them to protect it
- Nearly **20%** of employees don't feel confident their employer will take care of them, leaving them to actively seek other employment
- Of businesses who received identity theft-related attacks, like phishing, **40%** reported employees' workplace actions were significantly disrupted
- **35%** of businesses said identity theft-related attacks lead to the loss of productivity for employees, and an additional 8% said this damaged their company's reputation
- When employees have their identities stolen, they can become easily distracted at work due to the tremendous financial and legal burden placed on them:
    - Victims of "New Accounts" fraud report criminals used their information to collect over $10,000 worth of goods and services
    - It can cost around $1,500 out of pocket to resolve issues stemming from identity theft
- In addition to being distracted, you can also expect your employee to miss a significant amount of work. The average amount of time to fix identity theft is 200 hours, and this normally takes around six months to finalize. But, for some victims, it can take thousands of hours and years of work before the problem is fully resolved

- This on-the-job distraction and missed work will eventually lead to employee disengagement, which can bring about severe problems for your organization, especially if multiple employees are involved. Gallup's annual State of the American Workplace 2016 report found companies with low levels of engagement, when compared to companies with high levels of engagement, experience

  - 20% lower sales
  - 17% less productivityfrom identity theft
  - 21% lower profitability
  - Between 24% - 59% higher turnover
  - 70% more employee safety incidents

Protect Your Assets

Willis Towers Watson predicts identity theft protection, offered by 35 percent of employers in 2015, could double to nearly 70 percent by 2018, which would make it the fastest growing type of employee perk over the next couple of years.

With a number of "solutions" on the market, it's imperative you select a plan that goes far above and beyond traditional credit monitoring services. Make sure the plan you select contains the following features, all of which come standard with InfoArmor's PrivacyArmor®:

- Proactive alerts **that notify** on applications for credit cards, wireless carriers, utility accounts and non-credit accounts
- The monitoring of **high-risk identity activity** such as password resets, fund transfers, unauthorized account access, compromised credentials, address changes and public record alerts
- Tools to assist in monitoring and preserving **your online reputation** across social networks
- A **dedicated advocate to guide** and manage your employees' full recovery process, restoring credit, identity, accounts, finances and their sense of security, in the event identity theft does occur
- A **$1,000,000** Identity Theft Insurance Policy to cover lost wages, legal fees, medical records request fees, CPA fees, child care and more without the need to spend countless hours away from work

For a full list of features your plan should include, visit here. And, if you're serious about protecting your employees' identities and finances, reach out. We'd love to help get you started.

Sources:

1. Federal Trade Commission
2. Society for Human Resource Management
3. Insurance Information Institute
4. CNBC
5. HR Hero
6. Access Perks
7. Dark Reading
8. Alien Vault
9. Wombat Security
10. Norton
11. Gallup

InfoArmor

InfoArmor, Inc.

7001 N Scottsdale Road, Suite 2020 Scottsdale, AZ 85253
Email: info@infoarmor.com

800.789.2720
www.infoarmor.com