

# Businesses Beware:

## Protecting Your Company from the Consequences of Workplace Identity Theft

**Did you know that, as a business owner, you could be found guilty of stealing someone's identity without even knowing it?**

The scary truth is that your business could be liable if identity thieves were able to access sensitive information because of lax company identity theft and security prevention practices.

Any business that handles private data is subject to the perils of identity theft – even if it's not your identity in jeopardy. It should be part of every business owner's due diligence to protect sensitive information -- and save your company from crippling lawsuits, customer breaches of trust, and potential fines for not doing so.

These are the same measures that are required to meet compliance issues, too, so if you make these standard practice as part of company policy, you'll be covered on multiple fronts.

Regulations like the Gramm-Leach-Bliley, HIPAA, FACTA (Fair and Accurate Credit Transaction Act), and the "Red Flags Rule" mandate how businesses handle private data, and non-compliance laws carries strong consequences, including pricey fines, criminal and civil litigation, and even prison time.

These consequences can also effect management and board members

-- both of whom are also subject to both civil and even criminal liability, since many laws hold them personally accountable if a company hasn't established policies and training.

Consider that the Texas State Attorney General's office assessed fines to more than 15 large and small companies in just the last year – fines that have now exceeded millions of dollars – for not having policies in place to protect employee and customer personal information.

### Dispelling misconceptions

One of the big misconceptions about identity theft is that it is mostly related to credit cards -- like stealing a credit card offer that didn't quite make it through the shredder, or stealing computer files by hacking into a company's system.

Another big misconception is that only people with good credit are targets for identity theft. It's easy to forget that we all have Social Security numbers, driver's license numbers, medical histories and more -- and that they're worth far more than just a credit card.



### Crucial steps to take now

**Every business should have an identity theft prevention program in place, that includes:**

- **Written policies about how your business handles non-public information such as social security numbers, HR records, credit cards and the like;**
- **A designated person who oversees that policy;**
- **Employee training about policy guidelines that include signed agreements of understanding;**
- **Notifying third-party vendors who handle your company's sensitive data that they are also expected to follow this policy.**

# Businesses Beware: Protecting Your Company from the Consequences of Workplace Identity Theft

However, the top cause is actually theft of records from employers, including any business that collects personal data from individuals – such as Social Security numbers during the hiring process. In fact, a report by credit information giant TransUnion found that identity theft from businesses is much more rampant – even trumping stolen credit cards or mail theft. Establish sound policies and procedures now -- and your business will be steps ahead of the curve.



## Be proactive now

As much as we try – and as much as we'd like to – we can't predict human nature. Send the positive message to employees, customers, clients and vendors that you care about protecting their valuable information.

Be proactive today -- and save millions in fines, increase customer confidence, and prevent headaches later. Not only will you retain the business you have, but you'll also attract new customers who will appreciate your proactive stance toward identity preservation and overall company security.

## Smart Resources for Your Business

The following are trusted resources every savvy business owner should have bookmarked, or filed away in a virtual Rolodex:

**FTC Guide:** A comprehensive overview for businesses on everything you need to know to set up an identity theft prevention program.

**Identity Theft Resource Center®:** A nonprofit, nationally respected organization dedicated exclusively to the understanding and prevention of identity theft.  
<http://www.idtheftcenter.org/>

**Privacy Rights Clearinghouse:** A nonprofit consumer organization with a two-part mission -- consumer information and consumer advocacy.  
<http://www.privacyrights.org>

**FTC's Identity Theft Site:** A one-stop national resource to learn about the crime of identity theft.  
<http://www.ftc.gov/bcp/edu/microsites/idtheft/>

## About the Author

Jason Lavender is a Certified Identity Theft Risk Management Specialist and the Managing Partner of Austin-based ID Theft Solutions of America (IDTSA). IDTSA specializes in protecting businesses from identity theft, including comprehensive risk assessments; formulating a written non-public information (NPI) policy; on-site employee training; and voluntary employee benefit programs. For more information, visit [www.idtsoa.com](http://www.idtsoa.com), or contact Jason at 512-814-0200, or [jlavender@idtsoa.com](mailto:jlavender@idtsoa.com).

Find IDTSA on  
The web at [www.idtsoa.com](http://www.idtsoa.com)  
Twitter via [@idtsoa](https://twitter.com/idtsoa) or  
Facebook at [www.facebook.com/idtsoa](https://www.facebook.com/idtsoa).



**ID THEFT SOLUTIONS  
OF AMERICA**