



Identity Theft in the Workplace and its Impact on HR


Identity Theft Facts



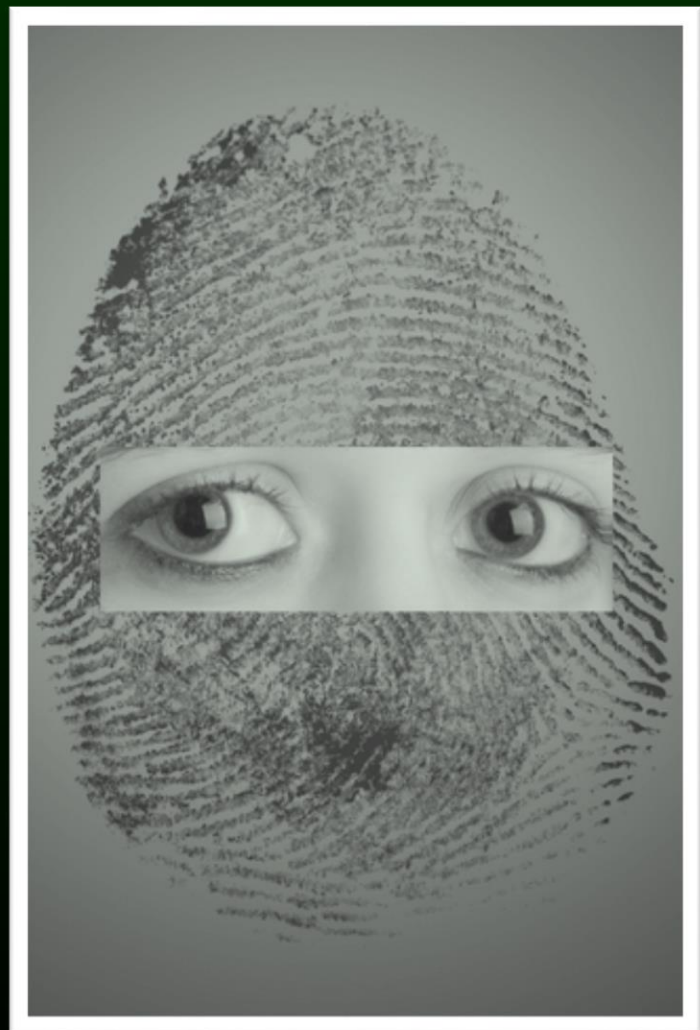


The Federal Trade Commission reports that identity theft has been the **NUMBER ONE** consumer complaint for **SIXTEEN** consecutive years!

ftc.gov

- In 2015, approximately 450 million records were compromised and 781 data breaches reported.
- Over 400,000 dead people opened bank accounts last year. 
- The revenue from trafficking financial data has surpassed that of drug trafficking. – *US Secret Service*
- Millions of children have reportedly fallen victim to identity theft.

- Last year produced the biggest increase in identity theft cases reported, jumping from 12.6 to 16.6 million.
- There are currently over 45,000 NEW identity theft victims **EVERY DAY!**
- Financial losses due to personal identity theft last year totaled 24.7 **BILLION** dollars...that is over 10 **BILLION** dollars more than the loss of all other property crimes.



- The average dollar amount charged in Identity Theft: **\$92,893**
- The average time taken by a victim to restore their identity is **607 hours.**
- Most identity theft issues are non-credit related.

How does Identity Theft impact employee productivity and your role in HR?

1. Absenteeism
2. Presenteeism
3. Data Breaches

1. Absenteeism

According to Forbes Magazine, “Absenteeism is an employee’s intentional or habitual absence from work. While employers expect workers to miss a certain number of workdays each year, excessive absences can equate to decreased productivity and can have a major effect on company finances, morale and other factors.”

1. Absenteeism

In a recent report, *Absenteeism: The Bottom-Line Killer*, it was stated that unscheduled absenteeism costs roughly \$3,600 per year for each hourly worker and \$2,650 each year for salaried employees.

1. Absenteeism

The bottom line: Absenteeism costs companies billions of dollars each year in lost productivity, wages, poor quality of goods/services and excess management time. In addition, the employees who do show up to work are often burdened with extra duties and responsibilities to fill in for absent employees, which can lead to feelings of frustration and a decline in morale.

2. Presenteeism

Presenteeism is defined as an employee being present but not being fully focused and productive because of personal health and life problem distractions. The old saying of someone "*being there in body only*" sums up the concept of Presenteeism. Presenteeism manifests itself in many ways, such as lack of focus, accidents and mistakes, interpersonal difficulties, poor work skills and production problems.

2. Presenteeism

- Presenteeism accounts for 61% of an employees total lost productivity and medical costs
- Some studies suggest that Presenteeism to be more than 7 times as costly to employers as absenteeism.

- Cornell University study, Journal of Occupational and Environmental Medicine

2. Presenteeism

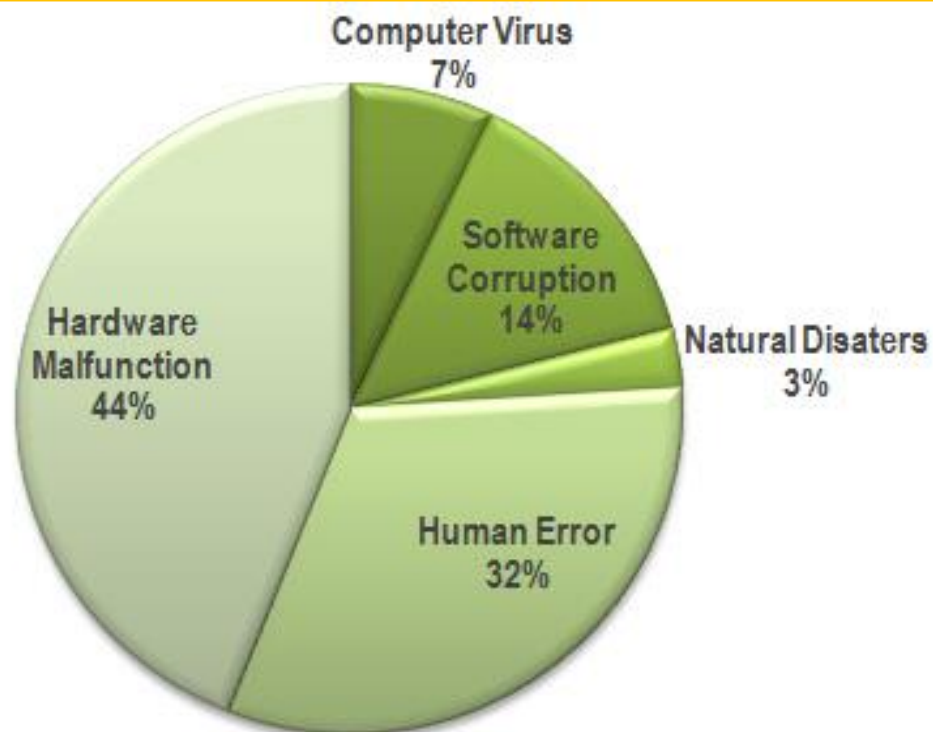
According to various studies, the total cost of presenteeism to U.S. employers falls anywhere between \$150 billion to \$250 billion each year, and those costs are on the rise as presenteeism becomes more frequent in tight economic times.

3. Data Breaches

The Ponemon Institute's ninth annual "Cost of Data Breach Study," estimates that the average data breach across the globe cost victims about \$201 per compromised record in North America last year, 9 percent more than the prior year

They also concluded that the average cost of a data breach rose 15 percent last year to \$3.5 million.

3. Data Breaches



Source: Ontrack survey

- If three of your employees told you that they have recently been a victim of identity theft - What does that mean to you?
- 32% of data Breaches are a result of Human Error

What can you do to assist your employees and protect your company?

- Educate them on the various forms of identity theft. Most of your employees are thinking that IDT has to deal with credit, but in reality only counted for 16.5% of all Identity Theft last year!
- Let them know how they can help prevent identity theft on a personal level as well as protect company information.
- Consider offering an employee benefit that deals in identity theft protection.

Common Types of Identity Theft





As a victim of
identity theft
you are **guilty**
until proven
innocent!





**Character &
Criminal**



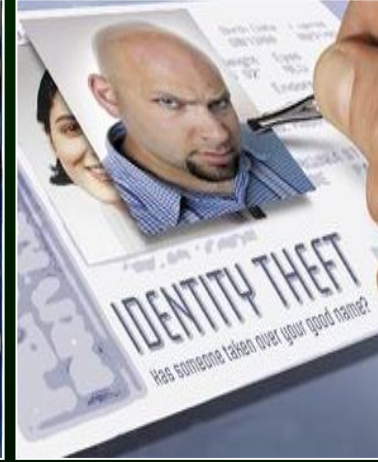
**Employment
SSA & IRS**



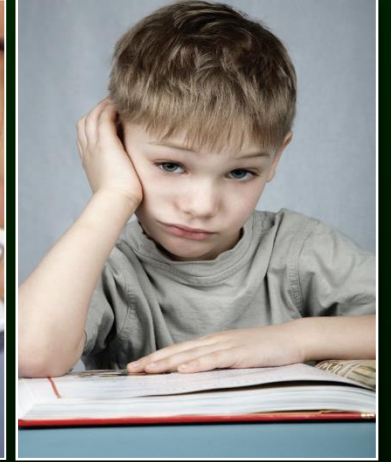
Medical



Financial



**Drivers
License**



**Minor
Children**





**Character &
Criminal**



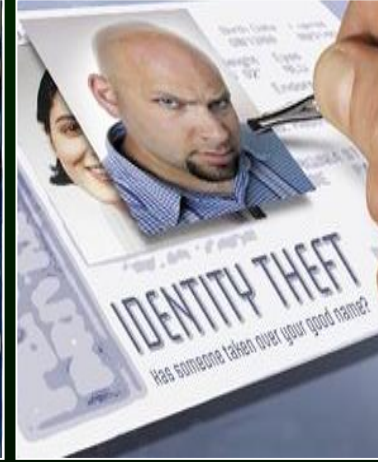
**Employment
SSA & IRS**



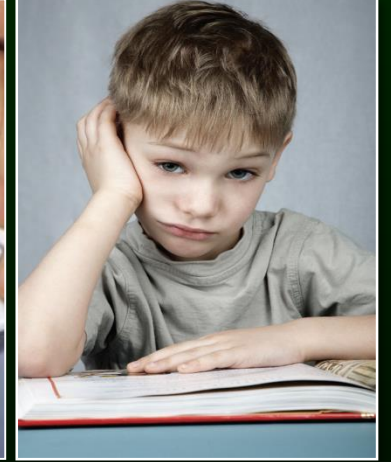
Medical



Financial



**Drivers
License**



**Minor
Children**







**Character &
Criminal**



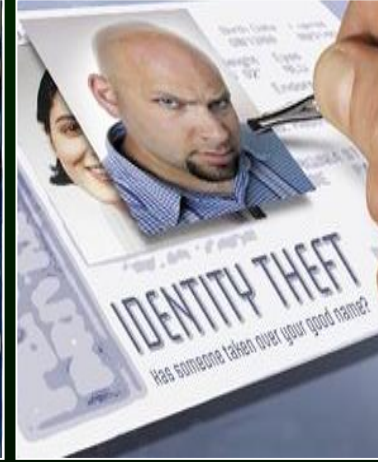
**Employment
SSA & IRS**



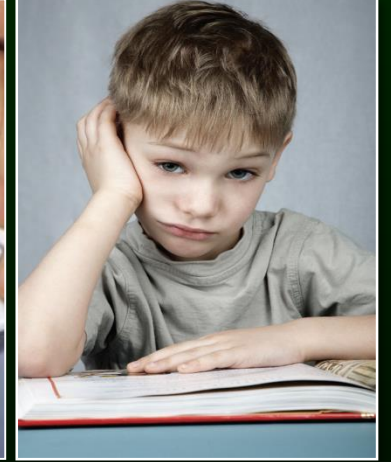
Medical



Financial



**Drivers
License**



**Minor
Children**



- A thief can destroy your good credit in a matter of hours.
- Average number of checks written in identity theft: 74.6
- Average number of credit card applications approved through identity theft: 8.4



**Character &
Criminal**



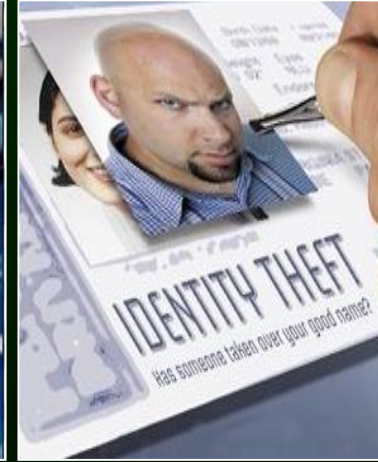
**Employment
SSA & IRS**



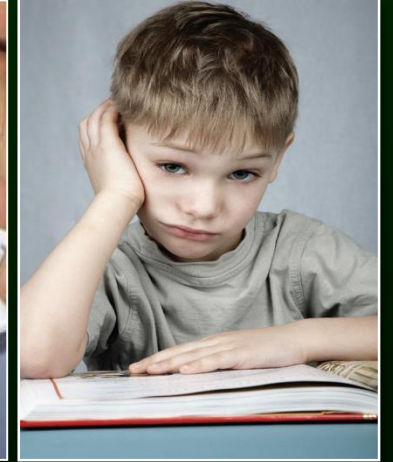
Medical



Financial



**Drivers
License**



**Minor
Children**



**Character &
Criminal**



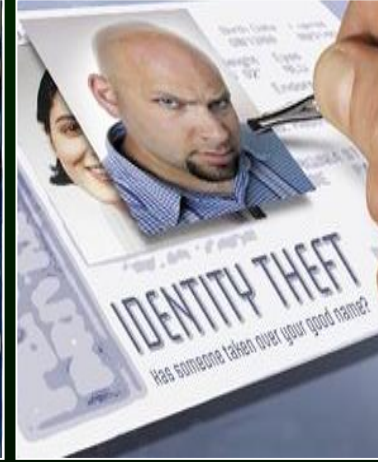
**Employment
SSA & IRS**



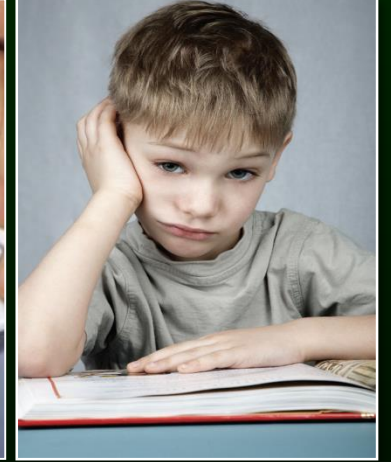
Medical



Financial



**Drivers
License**



**Minor
Children**



“I owe \$16,000 on my credit cards, my condo’s in foreclosure and I turn seven on Friday.”

- Millions of children have already been victims of Identity Theft. Of course, this is the number of discovered cases; the actual number may be much higher.
- Unfortunately many cases of Child Identity Theft are not linked to credit. Criminals are using children's identities to commit crimes, apply for Social Security benefits, obtain a driver's license, and even get medical treatment.







**Character &
Criminal**



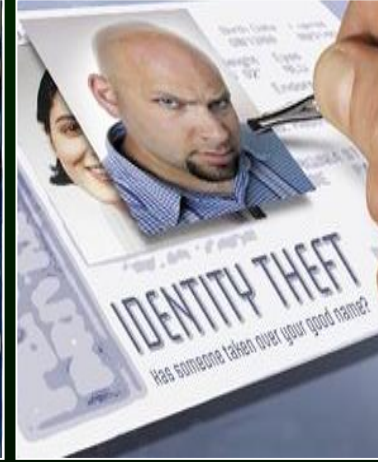
**Employment
SSA & IRS**



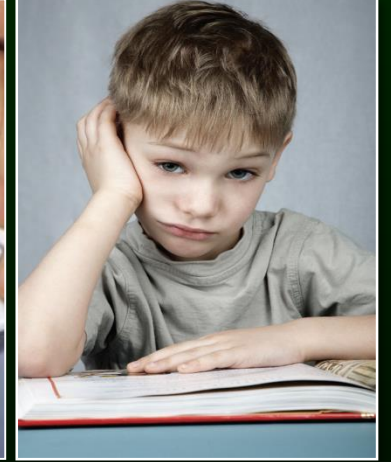
Medical



Financial

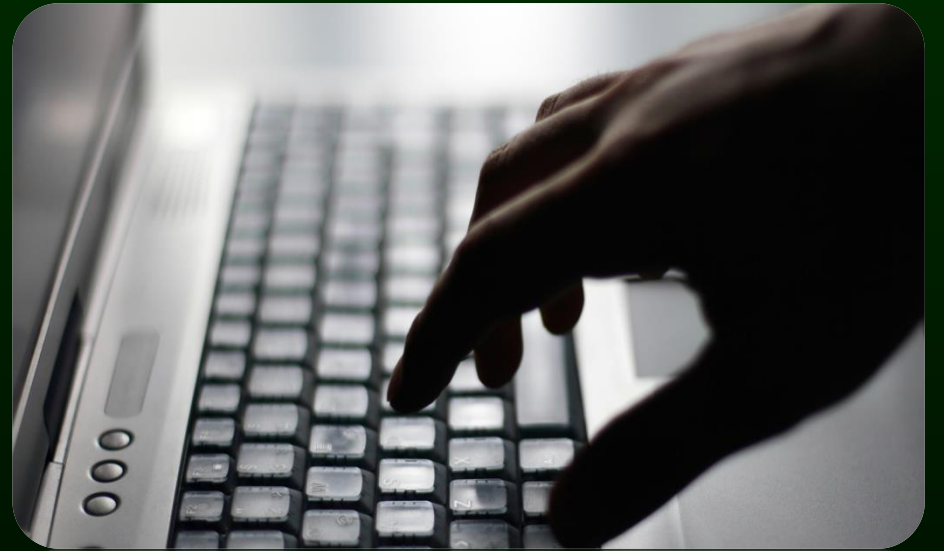


**Drivers
License**



**Minor
Children**

Current Identity Theft Dangers



Protecting Families, Finances, and Your Future

- **Phishing/Pharming** - Phishing occurs when thieves send out mass mailing/emails that appear to come from a legitimate source. Pharming is when a thief hacks an actual website and creates an identical duplicate site where victims unknowingly enter their information.
- **Skimming** - Now thieves can steal your credit card information and much more from inside your wallet! Unprotected smart phones are also a risk.
- **Caller ID Spoofing** - Thieves change the Caller ID to appear as a Sheriff's Office or Bank, then try to obtain information.
- **Data Breaches** - Many victims of identity theft today had their information compromised by a company losing sensitive information. Since 2005, over 900 million sensitive records have been compromised through data breaches.



- **Phishing/Pharming** - Phishing occurs when thieves send out mass mailing/emails that appear to come from a legitimate source. Pharming is when a thief hacks an actual website and creates an identical duplicate site where victims unknowingly enter their information.
- **Skimming** - Now thieves can steal your credit card information and much more from inside your wallet! Unprotected smart phones are also a risk.
- **Caller ID Spoofing** - Thieves change the Caller ID to appear as a Sheriff's Office or Bank, then try to obtain information.
- **Data Breaches** - Many victims of identity theft today had their information compromised by a company losing sensitive information. Since 2005, over 900 million sensitive records have been compromised through data breaches.

Notable Recent Data Breaches:

- Anthem (Blue Cross Blue Shield) - *80 million records* (Feb. 2015)
- JP Morgan Chase - *83 million records* (Sept. 2014)
- Home Depot - *60 million records* (Sept. 2014)
- Target - *40 million records* (Dec. 2013)

Identity Theft Prevention Tips

IDENTITY THEFT PREVENTION TIPS

**12
TIPS**



**TO HELP PROTECT YOURSELF
FROM DEVASTATING
EFFECTS OF IDENTITY THEFT**

Protecting Families, Finances, and Your Future

1. Review a current copy of your credit report.
2. Make sure you shred “junk mail” and unwanted credit card offers!
3. Opt out when you receive Privacy Statements – You must write them to stop companies from sharing your information.
4. Do not carry your Social Security Card – Keep it safe at home.
5. Do not carry extra credit cards.
6. Copy the contents of your wallet and store in a secure place.

- 7. Do not mail bill payments and checks from home. Use locked mailboxes.**
- 8. Do not print your Social Security number or drivers license number on your checks.**
- 9. Order your Social Security Earnings and Benefits statement and check it for accuracy.**
- 10. Examine charges on your credit card statements each month.**
- 11. Never give your credit card number or personal information over the phone unless you initiated the call.**
- 12. Invest in an identity theft protection plan that provides restoration services.**



Employee Benefit Plans

Protecting Families, Finances, and Your Future

Top reasons why employers offer identity theft plans as an employee benefit:

- The average identity theft victim can spend hundreds of hours in the process of restoring their identity.
- Many employees use their time at work trying to restore their identity and repair their credit.

- Identity theft protection is among the top voluntary benefit offerings to watch for employers, according to results from a Voluntary Benefits and Services Survey conducted by Towers Watson.
- At a recent benefits fair, 65 percent of employees surveyed indicated interest in either learning more about or signing up for identity theft protection.

- “The biggest reasons to offer identity theft benefits are lost productivity and employee stress, which, in turn, add to medical costs...the longer an employee doesn't realize that his or her identity has been stolen, the worse the damage becomes. It could take hundreds of hours to resolve...It's far better if an identity theft is found early in the process, and that's the goal of a good identity theft protection program.”

– *The Case for Legal and Identity Theft Benefits, SHRM*

- By offering an identity theft plan that includes credit monitoring as an employee benefit, businesses create an automatic early warning system for potential data breaches that may occur within the company.
- Plans that offer restoration services may also help to mitigate damages caused by a data breach.

Business & Legal Resources (BLR)

“One solution that provides an affirmative defense against potential fines, fees, and lawsuits is to offer some sort of identity theft protection as an employee benefit... have a mandatory employee meeting on identity theft and the protection you are making available, similar to what most employers do for health insurance.”

- *Top 10 Best Practices in HR Management (Special Report)*

The best part: Many plans can be offered at absolutely no cost to the employer. Your business can save money without spending money.



Most identity theft benefits are like hospital gowns...

You only **THINK** you're covered!



- **Monitoring Plans**
- **Reimbursement Plans**
- **Fraud Alert Services**
- **Restoration Plans**



It takes...

About
60 seconds
to find out
that you are a
victim of
identity theft

An average of
600 hours
to restore
your identity

When is the best time to act?

It is no longer a question of if your identity will be stolen - the only unknown is when it will happen.

- *ABC News*

“ It's just a matter of time. The cardinal rule of the identity theft quagmire is simply that, sooner or later, every last one of us will get got. No exceptions.

— *2016 Identity Theft: Fraud Hits an Inflection Point*



Identity Theft in the Workplace and its Impact on HR