



# Round Out Your Suite of Benefits With Identity Theft Protection

Identity Theft Protection Provides  
Peace of Mind to Employees and  
Protects Company Productivity

## **Introduction**

Every year nearly 10 million Americans have their identity stolen. The emotional and financial stress these victims face and the wake left behind is often overlooked.

With many kinds of identity theft from medical identity theft, tax fraud, to payday loan fraud, everyone in today's world is at risk for identity theft. It is no wonder that having one's identity stolen has become a top concern of consumers.

Employers are starting to take notice of the impact this up and coming crime has on employee performance. As a result identity theft is one of the fastest growing voluntary benefits being offered at the workplace. An identity theft protection plan not only provides the protection that employees need, it also adds value to a company's benefits offering and their cyber security plan.

## **How Data Breaches Can Lead to Identity Theft**

Over 500 data breaches were made public in 2017, including the Equifax breach. The Equifax breach alone exposed over 154 million records of personally identifiable information (PII). Despite companies' best efforts to protect the personal information of customers and employees, hackers are getting savvier and identity theft is becoming increasingly common.

No industry or market is immune to threats of identity theft. We have seen a rise in identity thieves targeting employers and consumers in education, medical/healthcare, government/military, financial/ insurance services, and retail. Data breaches have the potential to expose PII of every customer or employee that has or had a relationship with the breached organization. This includes information such as Social Security numbers, driver's license numbers, financial records, credit and debit card account numbers, medical records and more. Even what some would consider to be small pieces of personal information, such as an email address, can lead to identity theft.

Hackers profit from breaches by selling the obtained data through a series of websites where PII is sold and traded illegally, commonly known

## Common Types of Identity Theft Include:

- Tax
- Employment
- Government Benefits
- Medical
- Criminal
- Mortgage
- Fictitious Identity
- Utility

as the Dark Web. Some information is more valuable than others. For example, a comprehensive set of personal data that may include an individual's full legal name, birthdate, Social Security number, and payment card information may be priced between \$20-\$75 per record; a physical U.S. passport may be priced at up to \$5,000.<sup>1</sup>

Most people hear "identity theft" and immediately think of personal information being used for credit card fraud or to secure new lines of credit – and that does frequently occur. However, according to the most recent issue of the Consumer Sentinel Network Data Book published by the Federal Trade Commission (FTC), employment or tax-related fraud is the most common form of identity theft, making up more than one-third of the reported complaints in 2016. Thieves also use stolen personal information to set-up phone service and utilities, commit bank fraud, obtain government benefits, and pay for medical procedures or receive fraudulent prescriptions. Regardless of the form of identity theft, victims are left in a stressful situation that costs them time and money.

### Impact of Identity Theft

Identity theft takes a financial and emotional toll on its victims. This added stress can spread into the workplace and dramatically impact productivity and presenteeism. Depending on the type and extent of the identity theft, employees can take hours, days and even months, to resolve all the related issues. Tax Fraud for example, one of the top identity theft complaints in 2016, can take up to 6 months to resolve.<sup>2</sup>

To add to an already stressful time, the average worker may not know where to turn to dispute fraudulent accounts, clear collections, or to restore their reputation. This uncertainty adds to the emotional distress one experiences when they are a victim of identity theft.

**80.5%** of identity theft victims have experienced mild to severe emotional distress.<sup>3</sup>

It can take up to  
6 months to  
resolve tax fraud<sup>2</sup>



Tax-related  
fraud is the most  
common form of  
identity theft.


Employees already spend time at work on everyday personal financial issues<sup>4</sup> which is a distraction that impacts productivity. When navigating the process of restoring their identity, the problem is compounded and may even require time off work to resolve the identity theft matter.


### **Identity Theft Protection As An Employee Benefit**


Benefits packages are a competitive advantage for employers and have typically included services to protect the physical health of employees. In recent years, employers have evolved their suite of benefits to include protection of the financial and mental health of employees as well. Identity theft protection is a natural addition to the wellness portion of a benefits package. With today's diverse, multi-generational workforce, employers are often looking for benefits that will address the varying needs of employees. Identity theft protection fits the bill. When it comes to gauging the chance that one or more employees will be a victim of identity theft, it's not really a question of "if" but "when." Hackers and their "customers" aren't selective about whose information they steal, putting everyone at risk regardless of age, income, credit score or current financial state.

An identity theft protection plan is a proactive approach to protecting employee's identities and can also be a valuable addition to a company's cyber security plan. Employees are provided peace of mind that their identities are protected and the company's vulnerability is reduced when employees use company resources for their personal benefit, such as their email address and computer for banking or shopping. Similar to how health insurance won't prevent an employee from getting sick, an identity theft protection plan can't prevent identity theft from occurring. What it can and should do is offer assurance that employee's personal information is continuously monitored for misuse, that the employee will be notified right away if suspicious activity is detected, and that if they are a victim of a identity theft they remain focused and productive in the workplace and that they receive full identity restoration services.

While everyone's information may look the same to a hacker, identity theft protection plans are not all created equal. When considering adding an identity theft plan to their employee benefits program, benefit professionals should carefully consider the following features:

 **Continuous credit monitoring.** Clear signs of identity theft are unexpected changes to a credit report. Changes such as new credit, late payments, change of address or new employment could signal that an individual's personal information has been compromised. Even if the change is merely a reporting error, it needs to be addressed so as not to negatively impact the individual in the future.

 **Non-credit monitoring.** As mentioned earlier, not all identity theft is credit-related. A thorough identity theft protection offering should include monitoring of online sites and marketplaces for an individual's bank, debit and credit card account information, passwords, driver's license number, medical identification numbers, and more. In addition, a thorough service will monitor court records to see if a crime has been committed in the member's name, payday loan records to see if someone has used the member's personal information to obtain credit from a service that does not check credit reports, and social media profiles to see if a member is putting themselves at risk by posting personal information.

 **Consultative support.** An identity theft protection service is only as good as the ongoing support it provides. What happens if an employee receives an alert, or an offer that sounds too good to be true? What does it mean and who do they call? Employees should be able to reach out to an identity theft professional at any time who can tell them what an alert means and the next steps to resolve the matter. It is important to ensure the identity theft protection provider selected has experienced licensed private investigators, who are fully able to assist the plan participants with a variety of identity theft matters. Including how to recognize a potential scam and avoid becoming a victim of identity theft.



## With the IDShield Mobile APP, Participants Can:

- Directly Call a Licensed Private Investigator, 24/7
- Receive and Review Credit and Identity Threat Alerts
- Track Their Credit Score



**Full restoration.** Despite everyone's best efforts, the odds are great that one or more of a company's employees will become a victim of identity theft. This is when they really need a professional to take over and work their case. Employees should have a designated licensed investigator assigned to their case; one who will conduct further investigation to make sure all identity theft issues are identified, and resolved until the victim's identity is restored to pre-theft status.



**Additional features to consider.** A complete identity theft protection plan will include enhanced features that offer employees even more convenience, education, and support. Some features to consider:

- 24/7 emergency support
- Identity threat and credit inquiry alerts
- Mobile app for quick convenient access
- Password manager

IDShield is the only identity theft protection plan that provides direct access to licensed private investigators. These investigators have credentials that matter including:

- Certified Fraud Examiner (CFE)
- Fair Credit Reporting Act Certified (FCRA)
- Certified Identity Theft Risk Management Specialist (CITRMS)
- Certified Information Privacy Professional (CIPP)

Benefits managers have many options and plans to consider. An identity theft protection plan is a fitting complement to any financial, health and wellness program. They can protect employees from identity theft, reduce workplace distractions and lessen their anxiety over the well-being of themselves and their family in the event of a data breach or an identity theft incident.

## Bibliography

<sup>1</sup>Flashpoint, Analysis: Pricing of Goods and Services on the Deep & Dark Web, 2017

<sup>2</sup>IRS Identity Theft Victim Assistance: How It Works, January 2016

<sup>3</sup>Bureau of Justice Statistics Bulletin, Victims of Identity Theft, 2014

<sup>4</sup>An Employee Crisis: Financial Literacy, Purchasing Power, April 2016

IDShield is a product of LegalShield, and provides access to identity theft protection and restoration services through an exclusive relationship with Kroll. Neither LegalShield nor its officers, employees, or sales associates directly or indirectly provide identity theft protection, restoration services, or advice. A service of the Investigators of Kroll. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into a language or computer language, in any form by any means, electronic, mechanical, optical, chemical, manual, or otherwise, without the express written consent of Kroll. These materials are provided for informational purposes only.