WHITE PAPER

IDENTITY THEFT COSTS YOUR COMPANY MONEY – HERE'S WHAT YOU CAN DO ABOUT IT

The business case for identity management services

CYBERSCOUT™

INTRODUCTION

Identity theft is top-of-mind for most Americans, which means your employees understand the very real threat that it represents. Whether it's a financial loss or the emotional stress of salvaging credit standing, someone you know at work has very likely been a target of identity theft, and the individual damage it causes can be far-reaching.

But a recent CyberScout/BenefitsPro Survey revealed that it's not just victimized employees who suffer when identity theft happens. When their staff is defrauded, employers also are affected—and the impact may be deeper than many might expect.

A growing number of employees are taking time away from work to resolve creditor disputes, recover cash and tie up the myriad issues presented by fraud. This, plus the stress of identity theft, can lead to thousands of lost hours of employee productivity each year, depending on the size of the company. It's here that a proactive HR or benefits manager can make a difference by offering identity theft protection as part of a comprehensive employee benefits package.

UNDERSTANDING THE THREAT

Simply put, identity theft is a common occurrence. It's so common, in fact, that it is one of the top consumer complaints reported each year to the Federal Trade Commission (FTC) and other enforcement agencies. And a vast majority of HR and benefits managers—92 percent—know at least one employee who has suffered some form of identity theft.[1]

HR and benefits managers are uniquely positioned to help their employees understand the scope of the problem. Identity theft comes in many forms—from credit card loss and fraud to stolen checks and misused Social Security numbers—and it's smart to educate your staff about specific risks on a regular basis.

According to the FTC's 2017 Consumer Sentinel Network Data Book, tax fraud is the most common form of reported identity theft, closely followed by credit card fraud. Tax fraud occurs when someone files a tax return with a stolen Social Security number, then proceeds to claim a pending tax refund. Credit card fraud, on the other hand, comes when a stolen card is used to make purchases or obtain funds from another's account.

While these two fraud standards top the list identity thieves are finding many other avenues to your employees' sensitive financial and personal information.

- **Lost or stolen mobile devices**. Smartphones and tablets contain a considerable amount of personal data, from bank and credit card information to important and sensitive emails and messages. Identity thieves often recover personal passwords from lost and stolen devices, and they use that information to access bank accounts—or even purchase a new smartphone.
- **ATM card fraud**. Debit cards are a prime target for identity thieves as they can be used for unauthorized purchases and withdrawals. Sometimes, fraudsters attach card skimmers to a legitimate ATM machine, which then capture the card's magnetic strip data. These skimmers can be difficult to notice, leaving a great number of people open to this fraud.
- **Social Security or passport theft**. Identity thieves might steal a Social Security card or passport, forage through the trash for card and passport numbers, or obtain the information from a data hack online. No matter the source, once Social Security information is stolen, identify thieves can use it to apply for credit or claim government benefits. There's also a huge black market in stolen passports.
- **Check fraud**. Checks often are stolen from the mail, and that means an identity thief can use the information on the check to easily access your money. Identity thieves also might use "check washing" to commit check fraud, taking an existing check and altering it with new information.
- **Medical identity theft**. Health care providers keep considerable amounts of information about their patients, which makes insurance companies, hospitals and doctors prime victims of cybercrime. Medical identity theft may result in insurance fraud or even access to patient billing information, including credit card and Social Security numbers.

- **Cyber data hacks**. Americans rely on their smartphones, tablets and computers for work and leisure. Anytime personal information is online, however, there's the risk of exposing it to identity thieves. Some of their more common schemes include:
    - **Rogue apps**. Apps are ubiquitous: They give us access to bank and other account information, keep track of fitness and help us play the latest game. But with the good come the rogue apps that expose users to malware. Your employees might not necessarily be cautious in identifying fraudulent apps.
    - **Man-in-the-middle attacks and pharming**. Cyber data hacks can be sophisticated, like man-in-the-middle attacks, which intercept personal data sent from one legitimate party to another via the internet. Pharming occurs when a legitimate URL, such as a bank's website, is rerouted to a fake website mirroring the original one. Identity thieves count on unsuspecting victims/visitors to enter their personal information on the spoofed website, where it can be captured and used.
    - **Smishing**. Identity thieves also are stealing personal information via text messaging. Here, the identity thief sends a spam text message that appears to be from a legitimate source, such as a financial institution. The person receiving the text is likely to respond and provide their personal information.

DIFFERENT TYPES OF THREATS

Employees may have different points of exposure depending on their lifestyle, age and behaviors. Identity thieves, however, understand the public and their habits—and will take any opportunity to exploit them.

- **Millennials**. Younger workers grew up on their mobile phones. They live on their tablets, and they're accustomed to providing personal and financial information online. But the more time spent online, the greater the odds of identity theft. While millennials are tech-savvy, they aren't always as sophisticated about protecting their online data. They often use unprotected Wi-Fi, for instance, to transact personal business, and they're much more likely to use apps indiscriminately—both behaviors that can make them vulnerable to cybercrime.
- **Senior employees**. Your older staffers may have a much different profile. This group is likely to prefer written over online checks, along with receiving paper bank statements. With multiple accounts and often higher assets, senior employees may be open to even more damage than younger counterparts—compounded by the fact that it may take the older group longer to become aware of compromised financial or personal information.
- **The C-suite**. Identity theft might not be among company leaders' biggest concerns. However, the C-suite is at risk of incurring even greater loss with identity theft, simply because of their importance to the company and the importance of their full attention and presence.

HR and benefits managers clearly have some grasp of the problem's scope. This puts them in a unique position to help protect employees *and* the C-suite, and to educate at all levels. Identity theft protection solutions and services can help shield both employees and companies from the increasing threat.

A GROWING EMPLOYER CONCERN

This "employee problem" also is the employer's problem, though. The Federal Trade Commission notes that identity theft complaints nearly doubled between 2010 and 2015. That means that many more employees are spending increasing amounts of time resolving their own identity theft. The lost man-hours can be significant.

- Employers are increasingly acknowledging the threat. The risks are clear, and the problem is pervasive.
    - Ninety-one percent of C-level executives and HR professionals who responded to CyberScout's identity theft protection survey admitted that they are concerned about data and cyber security.
    - Eighty-six percent are concerned about identity theft.

- Data also indicate that most HR and benefits managers personally know employees who had been victims of identity theft.

Despite the evidence, however, employers are still failing to acknowledge the threat. Forty-seven percent say they discuss identity theft only once a year or almost never. And just over half are planning to or currently offer identity theft protection as part of the employee benefit package—which leaves nearly 4 in 10 (39 percent) that aren't likely to offer the protection at all.

Part of the problem? It may simply be that HR and benefits managers don't know how to start a discussion with senior leaders.

WHAT CAN YOU DO?

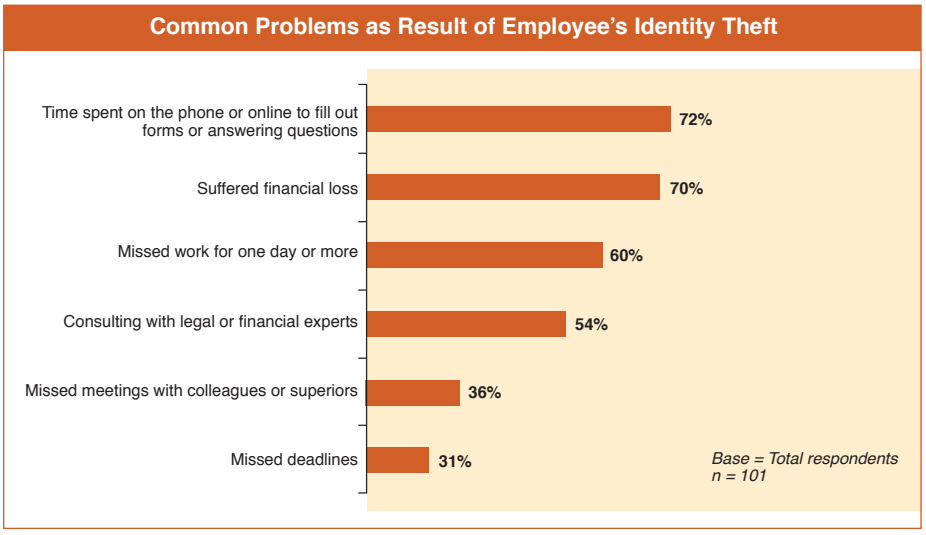
Before HR and benefits managers can make the case for offering voluntary employee identity threat protection, they'll need to spark a discussion. There is a clear need for a realistic conversation about identity theft protection among employees, senior leaders and C-suite executives.

- **A competitive edge**. Let your company decision-makers know that, in order to be competitive, employers will need to match their counterparts' offerings.
- **Getting buy-in**. While corporate IT professionals have long been aware of identity fraud protection, they can't necessarily effect sweeping employee benefits changes. Simply put, HR and benefits managers need buy-in from senior leaders in order to get the green light for offering identity theft protection as an employee benefit.

To make the case for identity theft protection, take a no-nonsense approach: Hit them in the pocketbooks. Senior leaders are much more likely to opt for a new benefit or solution if they can understand the employee value proposition.

THE BUSINESS CASE FOR IDENTITY THEFT PROTECTION

Identity theft is a very real productivity issue for employers—one that translates into dollars and cents. Respondents to the CyberScout survey indicated that roughly one in 10 employees have suffered tangible effects, primarily in the form of lost time (nearly one day in a typical work week) and money (nearly $500 on average). C-level executives and HR professionals identified a set of common problems that plague identity theft victims.



The need to understand the threat and to take steps to prevent it means HR and benefits managers have to take a proactive role in finding the right identity theft protection service provider.

THE SOLUTION: HOW PROACTIVE PROTECTION WORKS

It's imperative to take measures to guard against identity theft. Fortunately, more corporations are proactively protecting personal customer information, and many more businesses are recognizing the value of protecting their employees, too. HR and benefits managers are in the position to bridge any organizational knowledge gaps.

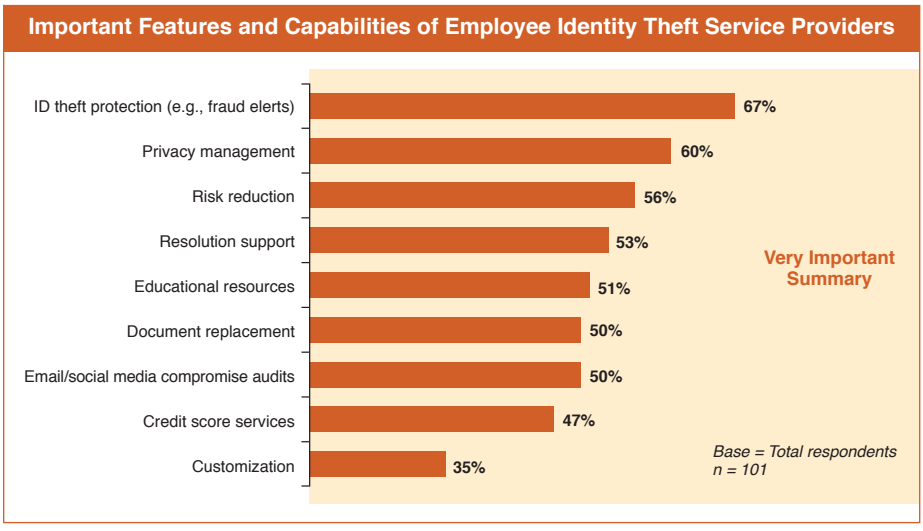
- **A deeper understanding**. Employers and employees, first and foremost, need more than a cursory understanding of identity theft and how solutions can help. Currently, most have a shallow knowledge of such a service: CyberScout found that only 32 percent of respondents admitted that they were "very familiar" with these solutions.
- **Knowing more**. Employee identity theft protection encompasses a variety of services and solutions. A good identity theft protection services firm will provide ID and data defense services that run the gamut from proactive protection and education to successful fraud resolution.

HR and benefits managers can make an even stronger case for such solutions with the right information in hand. With identity theft protection services in place, a data breach or fraud attempt is much more likely to be thwarted—or, if it does happen, detected early. And the best part is that, as a voluntary benefit, the offering comes at no cost to the employer—helping them save the man-hours lost by unproductive identity theft victim employees at no additional cost.

CONCLUSION

Whether it's an emotional and financial burden for employees or decreased worker productivity for the employer, identity theft is costing Americans and U.S. businesses considerable time and money. HR and benefits managers need to look for an innovative provider of identity protection solutions, recovery and breach services, as well as data risk management to address this ever-growing and evolving problem.

It makes sense to actively engage with identity theft providers to get a deeper understanding of their services and solutions and the robustness of their offerings. CyberScout survey respondents noted that they prefer identity theft service providers who can offer a wide variety of features and capabilities to their services and solutions.



Not surprisingly, identity theft protection can be a useful tool in attracting and retaining employees. By providing this valuable benefit, businesses are offering a major perk that will help you hire and keep the best and brightest employees on board. The next step for the smart HR or benefits manager is to find a trusted identity theft solutions provider to offer the best and most innovative services for their employees today and in the future.

1 All stats from the "2017 CyberScout Identity Theft Protection Survey," CyberScout, unless otherwise indicated.