



# Identity Theft: What it Means to Your Business

*Identity Theft is a concern for both consumers and businesses. How can you protect your employees, clients and customers from its debilitating effects?*

## **Introduction:**

In an era of rising crime, a wavering economy, and technological advancements, it's more important than ever to make sure that your business is protected from all angles. One such angle that is frequently overlooked is identity theft, which is generally defined as a fraudulent use of someone else's information without permission.

The identity theft epidemic is not new and the threat isn't showing signs of going away. As indicated by the FBI, identity theft is America's fastest-growing crime, and went up 23% in 2008 alone, according to a recent report by Javelin Strategy and Research. Given all of these scary statistics, the truly frightening aspect is the havoc that identity theft can wreak on an otherwise successful business or person.

## **ID Theft in the Workplace:**

In 2008, over 10 million Americans were victims of identity theft, and the numbers are continuing to rise. Some experts blame the poor worldwide economy, some point to rising technology, and others conclude that it's a combination of those and other factors. Whatever the reason, Americans find themselves at an increasing risk of becoming a victim of identity theft, and being left with all of the damage that comes along with such a crime.

For those unfortunate enough to be hit with identity theft, the damage can be overwhelming. While it may seem easy to cancel credit cards and receive bank reimbursement for lost funds, most Americans would be surprised to learn that only 20% of identity theft is even credit related. According to the most recent Federal Trade Commission (FTC) report, thieves may also use a victim's personal data to establish phone and utility accounts, obtain medical procedures, apply for jobs, forge government documents, commit crimes, and much more. For most victims, the damage has already compounded and reached several different avenues before they even realize their identity has been compromised.

As devastating as identity theft can be to an individual, the effects can cause even more headaches for the employer. In a study performed by the Identity Theft Resource Center, identity

theft victims reported an average of 116 hours rectifying the damage caused by the thief. On top of that, the study shows victims may spend thousands of dollars trying to restore their good name, all of which can over-run a victim's life. These efforts often lead an otherwise-dedicated employee to take excessive days off or even time on the clock trying to re-claim his or her identity. Employee focus and productivity can suffer for months and even years in light of being victimized.

## **Data Breaches:**

In recent years, identity theft in the workplace has become a disturbingly frequent trend, due in large part to the growing number of breaches to company databases. According to a Michigan State University study, the number one source of identity fraud is through theft of employer records, with 51% of identity thefts occurring in the workplace.

Any company that employs a staff is entrusted with a fair amount of personal information on every person that is hired or even considered for employment. Increasingly crafty hackers and developing technology have made data breaches an unfortunate reality for many companies, large and small.

In early 2009 alone, several notable data breaches were blasted all over the media, including that of the Federal Aviation Administration, in which 45,000 employees' records were compromised when a computer server was breached. Formerly, the FAA had been the model for other governmental agencies to follow with regards to security efforts. Also, in February 2009, over 30,000 Kaiser Permanente employees' personal data was found in a former employee's home. In yet another February incident, the University of Florida suffered a data breach when a hacker gained access to records containing highly sensitive data on students, faculty and staff.

According to privacyrights.org, over 260 million records have been compromised through data breaches since January 2005, and if recent history is any indication, this number will continue to rise rapidly. When employee data is compromised, thieves can use the information for any number of fraudulent activities,

# Identity Theft: What it Means to Your Business

including but not limited to large amounts of financial losses. Data may be sold to other thieves before the breach has even been detected, leading to a web of fraud that becomes virtually impossible for an employer or individual to untangle.

The effects of such a data breach can be devastating to a company. In addition to the money spent trying to rectify the damage caused to employees or customers, or lawsuits that inevitably arise in light of a security compromise, companies also must contend with the reputation damage that results. Working to re-build consumer and employee trust takes time, no matter how reputable the company's image was prior to the breach.

## Take an Active Role:

There are many preventative measures you can take to improve the security of your company's customers' and employees' private records. In fact, the Federal Trade Commission has mandated a "Red Flag Program" for any companies that handle financial information on behalf of their customers, which goes into effect May 1, 2009. This program outlines specific practices that companies must follow in order to keep their customers' private data safe. However, even if the Red Flag Program doesn't apply to your company, guidelines for keeping employees' records safe are also valuable in maintaining a successful company. For instance, if you use social security numbers on identification cards, paychecks, time cards or for log-in ID's, it is important to cease this practice immediately. Social security numbers are the keys to individuals' identities, and it is crucial that these be kept confidential.

Additionally, it is an employer's responsibility to shred all personal documents – including applications, résumés and cover letters – for all applicants that are not hired. Recently, a woman was charged with identity theft after obtaining hundreds of job applications, containing personal information such as addresses and social security numbers, from the dumpster of a local deli. Any documents that are not destroyed should be kept secure and confidential, with minimal employee access.

It is also important to educate your employees on the threat of identity theft, in order to protect themselves both in and outside of work. Individuals should closely guard their identifying

information and any personal records, and monitor their bank accounts and credit card statements for any suspicious activity. Shredding junk mail and being cautious about online transactions can also help consumers to guard themselves from potential identity thieves.

## Invest in Your Employees:

Although there are steps that you and your employees can take on your own to lessen your vulnerability to identity theft, there is no surefire prevention guarantee. Individuals are faced with an overwhelming number of outlets through which identity theft may strike, and cannot reasonably patrol them all on their own. What's more, if you have hundreds, even thousands of employees, it is nearly impossible to ensure their safety without some outside help.

Enlisting the services of an identity theft protection company, such as ID Watchdog, is a practical solution to making sure your company and employees are covered from the effects of identity theft. There are a number of ways that ID Watchdog, named by the Consumer Federation of America as being one of the most valuable services of its kind, is available to companies in a variety of capacities. Whether you choose to provide identity theft protection as a benefit to your employees, enlist the services of ID Watchdog Breach Protection, or a combination of the two, you can rest assured that you and your employees are covered by our comprehensive protection. Our patent-pending technology searches thousands of databases on behalf of you and your employees, ensuring that we detect any potential threats before they can compound.

Furthermore, ID Watchdog's resolution specialists will provide full identity restoration services in case any issues arise, either to your company's databases or to your employees. Our breach protection specialists will help you comply with Red Flag Program standards, and keep your employees' and customers' records secure. We will also help you establish a necessary contingency plan in the case of a security compromise. With all of the concerns you face in running a successful business these days, identity theft may be the last thing you expect to encounter. Give yourself and your employees peace of mind from this very real – and very damaging – epidemic today.

Please see [www.idwatchdog.com](http://www.idwatchdog.com) for more information on identity theft protection and breach protection through ID Watchdog.