

## IDENTITY THEFT PROTECTION AND RESTORATION SERVICES

### The crime defined

"**Identity theft**" refers to crimes in which someone wrongfully obtains and uses another person's personal data (i.e., name, date of birth, social security number, driver's license number, and your financial identity— credit card, bank account and phone-card numbers) in some way that involves fraud or deception, typically for economic gain (to obtain money or goods/services). Criminals also use identity theft to assume a fraudulent personality by obtaining ID cards, driver licenses, birth certificates, social security numbers, travel visas and other official government papers.

*"People don't understand that, in today's world, identity isn't just their credit identity – it's EVERYTHING."*

*-John Gardner Jr.*

*Certified Risk Management Specialist*

Although most people are familiar with financial identity theft, there are actually **five types** that are destroying American lives today – and the *"problem is sure to escalate with the economic downturn we are facing"* says expert W. Steve Albrecht, Associate Dean at the Marriot School of Management at Brigham Young University.

### 5 Types | Not 1



You may have never considered or even heard of a few of the identity crime categories above. None-the-less, financial represents only 28 percent of ID theft incidents, leaving you particularly vulnerable to the other four. Each type of identity theft can have devastating consequences for you, as the victim, who may face long hours of closing bad accounts, opening new ones, and repairing your wrecked credit record. And, it may take significant out-of-pocket expenses to clear your good name. In the meantime, you may be denied jobs, loans, education, housing, and cars, or even get arrested for crimes you didn't commit.

## Identity Theft in Real Life

ID theft is no longer an elusive, improbable nightmare. These stories illustrate real people with real lives that have fallen victim to identity theft while going about their normal, everyday activities. \*Names have been altered for privacy purposes.

*John was excited to close on his first home in beautiful Colorado. Confident in his ability to secure a terrific rate due to his impeccable borrowing history, he went to the bank to discuss loan options. Instead, he was denied financial assistance due to 4 foreclosures on in California – a state he had never lived in or visited. John was the victim of character identity theft.*

*Debbie was pulled over for speeding on the way to her son's little league game. Rather than a ticket or a warning, she was handcuffed and arrested for prostitution charges incurred 5 states away. Debbie was the victim of driver's license identity theft.*

*Steve went in for a routine physical exam at his South Carolina doctor's office. Upon check-in, his insurance denied payment due to significantly past due monies for extensive surgical procedures in Texas. Steve had never undergone surgery before. Steve was the victim of medical identity theft.*

*Melissa was a ten year veteran CEO with a publicly traded company. Financially, times had never been better! After a long day of board meetings, Melissa arrived home to a letter from the IRS stating that she had illegally evaded taxes last year and owed thousands for over 15 different reported jobs in four different states. Melissa was a victim of IRS identity theft.*

## The cold hard facts | ID Theft = America's fastest growing crime

FBI statistics and the Federal Trade Commission agree that identity theft is the nation's fastest growing crime. The FTC estimates that 10,000,000 people fall victim to identity theft each year. More than half of these Identity Theft incidents take place on the job and are due to human error. Criminals are targeting the workplace with new fervor as they have recognized the massive amounts of personal data stored on site or in files. Daily, employers and employees face invisible thieves completely unaware of the risk at hand and unprepared to protect themselves and their loved ones.

Identity crimes have taken the globe by storm because their perpetrators, unlike other crimes, are unseen. Perhaps sitting beside you at your favorite coffee shop yet conceivably across the globe or anywhere in between – ID thieves know no boundaries. As a result, most victims of identity crimes are unaware that their identity has been stolen until more than a year later. The implications are tragic. Families, businesses and dreams are devastated before any action is taken to bring justice; often it is too late. The best way to fight ID theft is to bring what is hidden into the light through awareness.

## Knowledge is your weapon

Awareness is one of the best defenses against becoming a victim of identity theft. Effective education entails not only what the crime and its risk factors, but most importantly, **your options for protection and defense**. The following information will equip you with the knowledge you need to protect yourself and your loved ones from suffering from identity fraud and a clear plan for restoration should you become a victim.

## How thieves GET your personal information

It is easy to think an identity crime won't happen to you – but that is far from realistic. As the statistics prove, thieves are getting smarter and, as a whole, we as individuals and companies are not prepared or protected against them. In addition, what we do know (or *think* we know) about ID theft is not completely accurate. So much attention is paid to credit card fraud occurrences; it's easy to assume that credit abuse poses the greatest risk to the victim/entity. That's not exactly true – your risk extends far beyond credit to the five types of ID theft mentioned above.

Because there are so many pathways into your personal data, protection is not easy to achieve. Despite your best efforts to manage the flow of your personal information or to keep it hidden, skilled identity thieves may use a variety of methods to gain access to your data. For example:

***Most victims are unaware that their identity has been stolen until more than a year later.***  
*Federal Trade Commission*

- **They get information from businesses or other institutions by:**
  - Stealing records or information while they're on the job
  - Bribing an employee who has access to these records
  - Hacking these records
  - Conning information out of employees
- **They may steal your mail, including bank and credit card statements, pre-approved credit card offers, new checks and tax information.**
- **They may steal your medical file from your Doctor's offices, Dentist, Chiropractor or even a Hospital.**
- **They may rummage through your trash, the trash of businesses, or public trash**
- **They may get your credit reports by abusing their employer's authorized access to them, or by posing as a landlord, employer, or someone else who may have a legal right to access your report.**
- **They may steal your credit or debit card numbers by capturing the information in a data storage device** through a practice known as "skimming." They may swipe your card for an actual purchase, or attach the device to an ATM machine where you may enter or swipe your card.
- **They may steal your wallet or purse.**

- **They may complete a "change of address form" to divert your mail to another location.**
- **They may steal personal information they find in your home.**
- **They may steal personal information from you through email or phone by posing as legitimate companies claiming that you have a problem with your account.**

### **How thieves USE your personal information**

As you have seen, there is a multitude of ways thieves can attain your personal information. Here are a few common criminal acts:

- **They may call your credit card issuer to change the billing address on your credit card account.** The imposter then runs up charges on your account. Because your bills are being sent to a different address, it may be some time before you realize there's a problem.
- **They may get medical care using your name or medical insurance card,** leaving you with unpaid medical bills or worse corrupting your medical files causing medical mistakes.
- **They may open new credit card accounts in your name.** When they use the credit cards and don't pay the bills, the delinquent accounts are reported on your credit report.
- **They may establish phone or wireless service in your name.**
- **They may open a bank account in your name and write bad checks on that account.** It's not uncommon for offenders to open multiple accounts in multiple places, and write bad checks on each.
- **They may counterfeit checks or credit or debit cards,** or authorize electronic transfers in your name, and drain your legitimate bank account.
- **They may file for bankruptcy under your name** to avoid paying debts they've incurred under your name, or to avoid eviction.
- **They may rent a house or apartment, and sign up for utilities, in your name.**
- **They may buy a car by taking out an auto loan in your name.**
- **They may get identification such as a driver's license issued with their picture, in your name.**
- **They may get a job or file fraudulent tax returns in your name.**
- **They may give your name to the police during an arrest.** If they don't show up for their court date, a warrant for arrest is issued in your name.

Although the methods of ID theft are diverse, the consequences have a common theme: stolen lives. The results are devastating and should be understood so that you can take proactive measures against theft as well as provide education or assistance to those you have a responsibility to care for.

**WHAT identity theft can mean for your life**

Below is A Russell Research study on common experiences suffered by victimized individuals. Note that in most categories, values have steadily and sometimes significantly increased over the past four years.

	2008	2007	2006	2005	2004
Denied credit	70.0%	64.0%	51.0%	60.0%	59.0%
Higher insurance rates	20.0%	14.0%	14.0%	17.0%	24.0%
Credit card rates increased	33.0%	36.0%	22.0%	30.0%	28.0%
Collection agencies still calling	39.0%	53.0%	46.0%	47.0%	43.0%
Credit card I had was cancelled	34.0%	27.0%	10.0%	19.0%	16.0%
Affects ability to get a job	23.0%	18.0%	12.0%	30.0%	16.0%
Unable to pay bills *	28.0%				
Lost my job *	5.0%				
Affects ability to get credit or a loan	45.0%	52.0%	63.0%	55.0%	68.0%
Affects ability to get tenancy	8.0%	14.0%	14.0%	17.0%	21.0%
Bad criminal record not cleared	6.0%	7.0%	8.0%	19.0%	10.0%

\* new categories for 2008

**A Stolen Life | How ID Theft affects you and your family**

Until you have been victimized, it is hard to understand the full impact of identity theft. The financial and other life-implications can be devastating to your business, your life and your dreams. However, the toll ID theft takes emotionally and mentally on you and your family cannot be quantified. In 2008, the Identity Theft Resource Center produced a report assessing the aftermath of ID theft from a pool of fraud victims. Below are some of the disturbing feelings victims suffered:

The experience of thousands of victims is that it often requires months, and even years, to navigate the frustrating, identity-recovery process.

*60% reported feelings of betrayal*

*21% reported a loss of innocence*

*37% reported feeling defiled*

*4% were suicidal*

*25% were "ready to give up the fight"*

*63% of victims felt powerless*

Moreover, entire families suffer from an identity fraud incident – not just the victim. Over 50% of participants said that their family life became stressed and over 21% said that their children also suffered as a result.

*In 2007 alone, cost to companies for data breaches was \$25 BILLION*  
-Ponemon Institute

## The Target | **WHO is at Risk?**

**Everyone.** Individuals, families, small businesses and massive enterprises are all at risk to suffering from an identity theft incident and its destructive repercussions. We have looked at the implications of identity theft at an individual level; now we turn to assess how the issue is affecting the business sector. There are multiple levels of risk that apply to businesses with the rise of identity theft. First and most obvious is the threat of sensitive information being leaked, much like an individual's financial information, directly damaging the company's bottom line. Large corporations often have the luxury of staffing their own legal team (e.g. General Counsel, Chief Security Officer, staff attorney) or can afford to outsource a legal firm for defense in the case of such incidents. However, thousands of small businesses exist largely unprotected against theft activity. For this reason, many small businesses are adopting small business plans that provide a system for defense through monitoring, restoration services and access to legal care.

Perhaps the more devastating risk in the longer term is liability. As mentioned earlier, the **workplace is now the site of more than half of all identity theft incidents.** Company data bases not only contain corporate records but can hold sensitive data on partners, buyers, suppliers, employees (and sometimes their families) and more. Should a data breach occur, all of this information is vulnerable to exposure. Now, company information alone is not the primary risk – but the organization faces **liability for damages incurred** to all parties involved. The financial implications are severe - monies paid out to repair identities compromised in a single breach are often in the millions of dollars.

This said, the intangible **damage to a company's reputation and brand cannot be measured.** Business exchanges are based, at their core, on trust. Once a company has been identified as "unsafe" they often suffer a massive exodus of current customers, struggle to acquire new customers, and face all difficulty in relationships with wary partners and other industry providers within their supply chain.

Recent legislature has brought new urgency to the table by issuing a mandate for businesses to take measurable steps towards protecting their employees and sensitive materials. In brief, if a data breach occurs and the company does not have a security plan in place, the government holds that company liable for damages done and may issue fines/other penalties against them.

This will ultimately prove advantageous to all parties involved as security becomes the norm but companies must take heed that they are in compliance with applicable legislation.

Below is a brief overview of the relevant laws and how they potentially affect business owners and executives.

**Fair & Accurate Credit Transactions Act (FACTA)\*:** Applies to every business that collects or maintains consumer information for a business purpose. Employee or customer information lost under the wrong set of circumstances could result in:

- Federal and State fines of \$2500 per occurrence
- Civil Liability of \$1000 per occurrence
- Class Action lawsuits with no statutory limitations
- Can be held responsible for actual losses of individuals (\$92,893 average loss)

**Gramm Leach Bliley Safeguard Rule (GLB)\*:** Applies to any organizations that collects or maintains personal financial information about its clients or customers. Information lost under the wrong circumstances could result in:

- Fines up to \$1,000,000 per occurrence
- Up to 10 years jail time for executives
- Removal of management
- Executives can be held liable both criminally and civilly

**A Multitude of State Laws:** There are now 35 states that have their own laws regarding identity theft and information security.

### **Life Happens. Are you and your Employees Protected?**

Life has its way of serving up crisis when we least expect it.

Answer the simple questions found in Appendix A for insight into the risk probability you or your company face. The first step toward defense is proper understanding of the risks you are up against. This is where protection begins.

## Proactive Protection | **A solution to the ID theft outbreak**

### **Identity Shield** ID theft protection and restoration services

In the world of business competition, successful and sustainable companies have a few key traits in common. An ***innovative approach to challenge*** is among them. Today we are faced with an escalating global economic crisis that many experts say is second only to the great depression. We have already seen the demise of several corporate giants and morale is steadily plummeting. Small businesses and large corporations alike face a critical decision: will they continue doing business as usual, hoping that their efforts will be sufficient to weather the storm, OR will they reinvent themselves and their products/services to meet the new demands of their consumers in today's market?

As a relevant and growing concern facing America's workforce NOW, the identity theft outbreak poses an incredible opportunity for companies to demonstrate the value they place on their employees by providing protection and promoting a security culture. There is real demand for an employee benefits option that would provide both defense against and assistance with identity theft.

Several ID theft options currently exist in the market; many companies have adopted them. However, few such options are truly effective tools to prevent you from becoming a victim. A proactive and valuable approach to the problem of identity theft will mean that you are not only alerted to a problem once it strikes, but have access to legal counsel to secure yourself and loved ones against a crime, a responsive alert system when an incident is recognized and, most importantly, a skilled team of experts to fight for full restoration on your behalf. In addition, this solution must be simple to understand and administrate.

### **Access to Counsel**

**Affordable access to quality legal care is a fundamental step towards protecting yourself and your family, your business and your employees.** Through sound counsel, many costly mistakes can be avoided, security measures put in place and peace of mind attained by knowing that you have legal resources on your side and an effective gameplan in place should a crime occur.

### **Continuous Monitoring**

You can rest easy and live life to the full knowing that our licensed investigators are watching your credit and other sensitive personal information. If an unusual act appears, you will be alerted and a recovery investigation begun in the case of a criminal action.

## Restoration Services

Monitoring alone can be likened to an emergency operator detailing HOW your house caught on fire rather than sending an emergency response team to fight it. Once you have been victimized, you need trained experts to help you fight the roaring flames rather than a service that simply alerts you to the problem.

**Credit monitoring alone  
is an inefficient and  
ineffective answer to an  
ID theft crisis**

## Simple, Meaningful & In Demand = **VALUABLE**

For a benefits option to be truly valuable, it must hold value for both the employer offering it and of course, the employees as the end-user. Based on this understanding, a valuable benefit is one that is simple to administer and service, meaningful to the real-life needs of employees, and in demand or needed by those it is intended to benefit.

What if there was a way to offer your employees a benefit option that was relevant to the real life issues they face and would act as an incentive to promote loyalty, decrease turnover and demonstrate your concern for the *whole* employee? Better still, what if this same benefit considered your need for a cost-effective and hassle free enrollment and service process? That would be a truly valuable service - one you should not live without.

As we have seen, the market **demand** for an identity theft shield is escalating rapidly as the crime grows at astonishing rates. Never before has demand for this benefit been so high. As a result of the crimes prevalence, an identity theft benefit is extremely **meaningful** to employees; it intersects with a real need that they either have or most likely will face. The bottom line is that employees are seeking this benefit out because it will mean something to them and their loved ones financial well being and peace of mind.

Finally, an effective identity theft protection service should be simple. As employers, you have enough issues on your plates. The last thing you need is more extensive paperwork, complicated forms, hassle, and other issues. We bring you our exclusive success system right to you. This system will be a customized solution for your company that will provide on-site training and enrollment as well as an administration process as easy as 1, 2, 3 to get your employees shielded right away.

## On Site Enrollment

At your convenience, a trained representative from Premier Solutions Intl. will make an onsite visit and conduct benefits briefings and enrollment session(s) for you.

### Simple Administration

At Premier Solutions, our Identity Shield benefit is simple and straightforward yet it expresses genuine concern for the well-being of the employees and companies we service. We understand how difficult benefits administration can be, so we've made it easy for you.

- **No long-term contract**
- **No claim forms**
- **No deductibles**
- **No time consuming administrative duties**
- **No cancellation forms**
- **Once a month billing**
- **Electronic enrollment and paperless billing options**
- **One rate for any size family**
- **Portable benefits**

Your employees simply enroll by completing the application and their **coverage begins immediately.**

Identity theft continues to be a problem in America, and everyone's at risk. The good news is your business and employees don't have to fall victim. **You can fight back.** Be prepared and proactive by raising your Identity Theft Shield!

## APPENDIX A: Test Yourself

Gauge your current knowledge of how to protect your identity and learn where your greatest risks may be.

1. When you receive an unsolicited offer of a “pre-approved” credit card in the mail you:

- a. Shred it
- b. Throw it in the trash, unopened
- c. Open the envelope, then throw the contents in the trash
- d. Use the envelope to send back other junk mail

2. What do you do if an expected credit card bill does not arrive?

- a. Suspect it was intercepted and call the credit card company
- b. Figure you got off easy that month
- c. Calculate how much you think you owe and send a check
- d. Wait a couple of weeks and see if it shows up

3. How often do you check your credit reports?

- a. Every time I apply for a loan
- b. Whenever I feel like it
- c. I check my credit report regularly
- d. What’s a credit report?

4. When you send mail, do you:

- a. Put it in the mailbox and raise the red flag the night before
- b. Put it in the mailbox and raise the red flag in the morning before leaving for work
- c. Ask your neighbor to drop it off since he passes the post office on the way to work
- d. Drop it off at the post office yourself

5. At this moment, where is your social security card?

- a. In my wallet or purse
- b. In my glove compartment
- c. In a secure location at home
- d. At my mother’s house, I think

6. How often do you check your credit card statements?

- a. As soon as the statement arrives
- b. Just before paying them
- c. I check them online from a secure computer

d. Whenever I get around to it

7. How often do you balance your checkbook?

- a. Once a month
- b. Every quarter
- c. Once a year
- d. I wait until the bank sends me a notice that says I am out of money

8. Where do you keep your financial records in your home?

- a. In a locked safe
- b. On the nearest flat surface
- c. In a file cabinet
- d. In an unlocked safe, since you can't remember the combination

9. When you select a computer password you use:

- a. Random letters and numbers
- b. Your mother's maiden name
- c. Your pet's name
- d. Your birthday

10. Where do you store your computer passwords?

- a. I tape them to the computer monitor
- b. Upper right hand drawer under a book of matches
- c. I memorize it
- d. In my wallet

**CORRECT answers:**

- 1. A
- 2. A
- 3. C
- 4. D
- 5. C
- 6. A
- 7. A
- 8. A
- 9. A
- 10. C

**Your score:**

**5-10 incorrect:** you are a prime candidate for disaster

**3-4 incorrect:** you have plenty of room for improvement

**1-2 incorrect:** Good, but you still need to tighten up things

**ALL 10 correct:** Excellent! But stay vigilant because you can still become a victim of identity theft