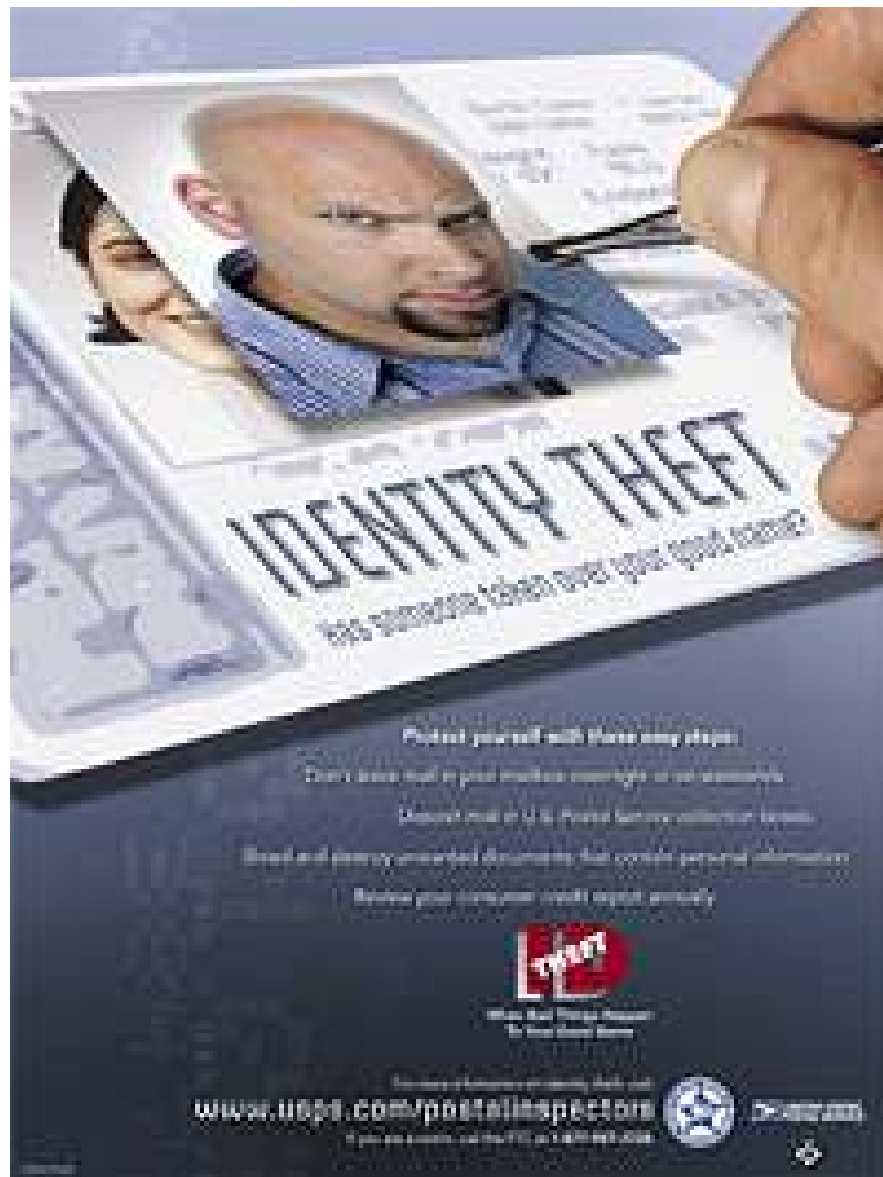


# Identity Theft

## How to Manage the Risk



Poster from the Postal Service

It's no secret: **Identity Theft** is a major problem in America.

Think you're not at risk? Unfortunately you are.

- Do you hand your credit card to servers at restaurants?
- Do you sign your credit cards?
- Do you supply personal information over the Internet?
- Do you keep your Social Security number in your wallet or purse?
- Do you leave mail at your home or business for the postal carrier to collect?
- Do you shred unwanted mail with personal information?

**The answer is knowledge and that is what I am going to share with you . . .**

## Introduction:

Look at what you do every day. You write a check at the store, go to lunch with a friend, charge a gift on your master card, rent a car, make calls on your cell phone, open a bank account, order checks, apply for a credit card, etc.



Most people do these things with out any thought to how or what happens to the information they provide. But, there is a danger that most people are not aware exists. A thief can get the information and use it to impersonate you without you knowing about it until it's too late. Criminals simply do not want to get caught or get punished. That's why they will impersonate you, commit crimes or money then leave you holding the bag. It suddenly becomes your responsibility to *prove* to the world that it was not you who committed those crimes. Worse, criminals can wreck havoc on your credit that may take a long time to recover.

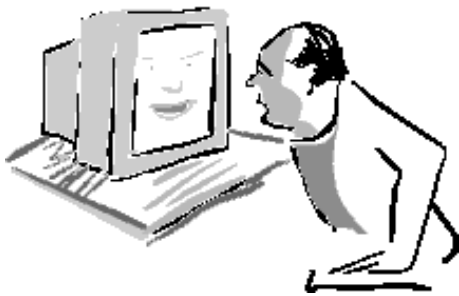


If you think that this could not happen to you, it already happened to **10,000,000** people in **2003** alone and is expected to **rise** in 2004, 2005, etc.

Our intent is not to scare you, it is to alert you and educate you. Even though this problem is widespread, there are many things every person *must* do to *reduce* the risk of *Identity Theft*.

## How did we arrive at this situation?

Information gathering, storage, analysis and retrieval have been occurring for a long time. From clay tablets to animal skin to paper, information is recognized as a valuable source for decision making. Stored information, however, is difficult to manipulate and analyze when it is stored on



paper. The development of the electronic computing machine gave a new meaning to information analysis. As these computers improved in speed and storage size, businesses found ways to gather and store information for “*later*” retrieval and analysis giving birth to “*The Information Age*”.


Information by itself has no value because raw information is simply “data”. What people do with information makes it either valuable or worthless. The result is that businesses make decisions based on the information they obtain regardless of accuracy.

Two major events occurred which made information gathering, storage and analysis more profitable and practical in the USA.



The first event that brought us to this point is the Social Security Act. On August 14, 1935,

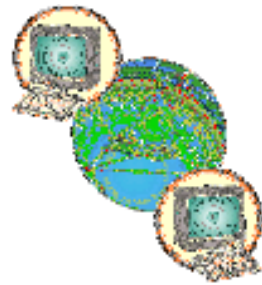
President Roosevelt signed the Social Security Act which allowed the creation of a national database to monitor financial contributions and tax collections for each individual residing in the United States. By law, the Social Security Number was not and is not intended to be used as an identifying number. Nevertheless, governmental agencies and private enterprise realized that technically no two individuals have the same SSN. Therefore, they adopted the SSN as an identifying number to track information about tax payers, customers and citizens.

How does all this relate to credit? In the beginning, when people bought goods on credit from the local store, the store owner or clerk tracked that information on a piece of paper or in a book. Eventually,  someone had the idea that the information collected is valuable for future credit references. The data collected may have included character references, insurance information, employment information and even driving records. There was no consistent way to verify that information and the customer did not even know what information was kept. Customers had no access to the information while merchants did.

The earliest known third-party credit reporting agencies date to the 1830's. They collected information from various sources and sold it to anyone for a price. These agencies had to compete with one another, serve their clients (Banks, merchants, credit grantors, etc.) and the general public. Their loyalty rests with the group that pays the bills; banks and merchants.

The one common thread these agencies use to tie all the data together is the SSN. Again, even though the SSN is not intended to be used for identification, it is being used along with the birth date and address for identification.

The second event is the development of the electronic computing machine we now call “The Computer”. Data storage, retrieval and analysis became more practical and profitable using computers. The one major development in the computer business that made data readily available is the Internet. It all started in the mid 1960’s with the creation of the pre-Internet network and culminated in the expansion of the present-day Internet. As more commercial enterprises, government agencies, financial entities and a hoard of others embraced the Internet; information became the currency of the new economy.



So, you ask, what does it all mean and how does it relate to *my* information? The answer lies in the *way* information is collected, tabulated and reported by businesses, government agencies and financial institutions.



You see, information is used by people to make decisions. Good information will most likely produce better decisions. Bad information will definitely produce bad decisions. Information in the right hands is fine as long

as that information is protected and kept safe at all times. Information in the wrong hands is bad for your personal and financial health.

The law requires that credit history information kept by credit reporting agencies be reasonably accurate and that the consumer has the right to access and dispute that information. The burden is placed on the consumer to monitor and manage his credit history. What this means is that unless you are diligent and keep a constant watch on your credit history, inaccurate, false and misleading information can find its way into your file. If that happens to your records, you are responsible for:

- Discovering the mistakes,
- Disputing the mistakes,
- Getting the reporting agencies to correct or remove the mistakes.

Take this situation a step further and consider what a thief can do to your good name and credit leaving you holding the bag for months or even years.

How do these thieves steal your identity anyway? It is easier than most people realize. The information thieves use is readily available.

## How Identity Theft occurs

Identity theft can happen to anyone. It used to be that a thief will steal your wallet for the cash. Now a thief will steal your information and take over your identity without getting close to you or even knowing what you look like.

This is how it may happen:

**Scenario 1:** You visit a local restaurant with a friend for dinner. You have a great time, eating, drinking and laughing for hours. Later, the waitress comes over with the dinner check. You hand her your trusty Platinum credit card then she walks away to the waitress station to “*process*” your card. When she returns she hands you the card and the charge slip to sign. You sign the ticket, leave her a big tip then go home. All seems normal because you’ve done this many time in the past.



The truth is you don’t know what happened to your card from the moment it left your sight to the moment the waitress returned it to you. Do you? Cloning a credit card takes seconds. Unfortunately, it is a well-known scam that some unscrupulous restaurant staff will copy your card by swiping it twice: once through the payment machine and once through a palm-sized electronic device which records the information on a magnetic strip for later retrieval and card cloning.

Let's not blame only restaurant workers. Anyone who takes your credit card to process an order can clone your card if he has a card reader. It is easy to hide a palm-sized card reader. A well trained thief will clone your card right under your nose without you noticing.

Card cloning is only one method for thieves to steal from you. A more prevalent method is to steal your information, create identifications with your information and his picture then open credit card accounts, bank accounts, store accounts and so on. All a thief needs is your name, SSN, date of birth and address. From there he can have a field day with your credit.



**Scenario 2:** You go to the doctor's office for a checkup. The office staff gives you forms and requests that you write down your name, address, SSN, date of birth, etc. You



comply and hand the papers back to the staff. The doctor's office is required by law to protect the information they collect about every patient. On the wall in the reception area, they display statements about their "*Privacy Policies and Practices*". You glance at the statements, read the statements and feel good that the doctor's office cares about you and your privacy.

It looks good on the surface. The problem lies in the actual practices of the staff and management at the doctor's office. Your information is kept in a paper folder and

entered into a computer at the office. Unless there are “*specific*” procedures to protect that information *and* the office staff follows these procedures, no statement tapped to the office wall will protect you. Dishonest cleaning crews steal information either from the paper files or from the computer. It’s estimated that around 60% of small to medium healthcare offices don’t use passwords on computer terminals. The information is right there for the taking.



**Scenario 3:** You get all types of credit card offers in the mail. You usually open the envelopes, read the basic offer,



and then toss the whole thing in the trash. Later that week, you leave the trash at the curb side for the waste management company to pick up. Is this wise? **NO!** You might as well have a sign on the trash inviting thieves to “*come and get it*”. Any

one will search your trash and find these offers that you threw away. He may also find the paycheck stub you threw away along with the old phone bills, electric bills, and credit card bills. In one visit he collects enough information to go to the next step. He’ll take everything.

He'll go home and sort things out. Skilled in his trade, he will create an identification card with your name, SSN, date of birth and *his* picture. Quickly he will become you. He'll complete the credit card offer with your name, SSN, date of birth and *his* address then sends in the application and waits. When the card arrives, he has access to whatever amount of credit the card issuer gave to him based on *your* credit. The thief will use this credit card, receive the monthly bills, and not pay anything on the bill then move on to the next victim when he no longer can use the card. Your name and credit take a nasty hit when creditors report delinquencies on your credit report. The worst part is that you will *not* know about this until the damage is already done when you want to buy a car, buy a house or get a student loan.



These are some scenarios but not the only ones. There are numerous possibilities and many ways for thieves to steal *your* information and impersonate *you* to steal money from you or in your name. There are even documented cases where thieves committed crimes, got caught and presented false identification in victims' names. In 2003 about 10 Million individuals were victims of Identity Theft in the US alone.

**Don't be a victim.**

**Act now to protect yourself.**

## How Identity Thieves Get Your Personal Information:

- They steal your mail from your mail box.
- They divert your mail through the post office.
- They steal your wallet or purse.
- They search through your trash or the trash of businesses looking for personal information. This is called “dumpster diving”.
- They obtain your credit report through the many online services by posing as a legitimate business.
- They get the information through the Internet.
- They scam you through e-mail.
- They get the information from work.

## **What You MUST Do**

As dire as it sounds, there are many things you must do to protect yourself, your money, your name and your family. You should have three aspects to your plan. Keep in mind that protecting your identity is NOT a one time shot but a continuous project. Once you have your plan in hand, you will spend a minimum amount of time monitoring it. Here are the three items:

- Prevention – minimize your risk
- Monitoring – keep an eye on things
- Response – quickly restore your name

## **Prevention – Minimizing Your Risk**

**Next three pages have check lists. Use them to close any loop holes in your system.**

**Signup for Identity Theft Shield™  
Call (913) 206-7209**

**If you have Internet access, go to:**

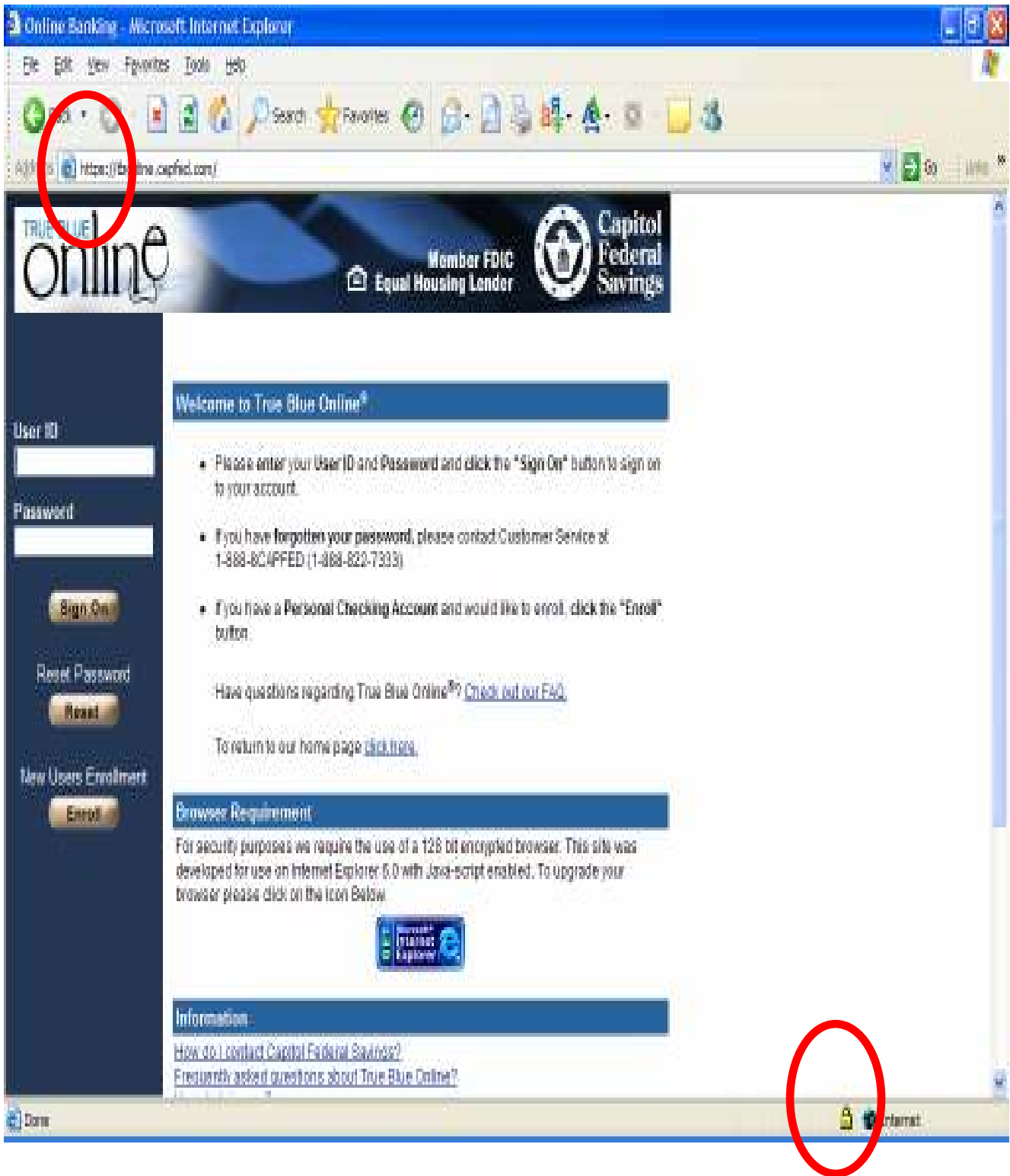
**[www.GTechAssociates.com](http://www.GTechAssociates.com)**

**Follow the links to sign up for Identity Theft Shield™.**

<b>Action Item</b>	<b>Check</b>
<b>Carrying Sensitive Information</b>	
<b>Memorize</b> your social security number then <b>leave</b> your Social Security Card at home in a secure place.	
Carry only “ <i>Must Have</i> ” identification cards and credit cards.	
<b>Memorize</b> passwords and PIN’s (Never carry them with you on paper).	
<b>Financial Transactions</b>	
<b>Leave</b> your checkbook at home in a secure place.	
Pay with a <b>credit card, cash</b> or <b>debit card</b> .	
<b>Always take</b> your credit card and ATM receipt.	
<b>Shield</b> your hand well when entering your PIN anywhere even at the bank.	
Always be certain <b>you know</b> whom you are dealing with when ordering anything by telephone or online.	
Banking online or ordering online? Always look for the “ <b>https//</b> ” in the address bar and the <b>closed padlock</b> somewhere on the page. See figure 1.	
Always pay for <b>online</b> or <b>telephone</b> orders with a credit card, not a <b>debit card</b> or a checking account draft.	
Always <b>print</b> your online transactions. Paper is cheap. Ask for <b>confirmation numbers</b> when ordering by telephone.	
If you use checks, always <b>keep an excellent record</b> and <b>monitor</b> the check number sequence.	

<b>Action Item</b>	<b>Check</b>
<b>Keeping Record</b>	
Monitor your bank accounts weekly. You can do this online.	
Monitor your Bank statements. Monitor your account statements on a monthly basis to ensure they arrive at the scheduled time and there are no discrepancies.	
If you order credit cards, ask for delivery to the bank or rent a secure post office box. Do the same when you order checks.	
Keep track of the billing cycle for ALL your credit cards. You will know immediately when a bill does not arrive.	
Review your Credit report at least once a year for any inaccuracies.	
You may want to consider opting out of unsolicited credit offers. You can call 1-888-5-OPTOUT (1-888-567-8688) to opt out of receiving pre-screened credit card offers. All three major credit bureaus use this same toll free number.	
<b>Information Maintenance and Protection</b>	
Buy a good quality <b>cross-cut shredder</b> . Shred all documents with personal information <b>before</b> throwing them away.	
<b>Do not</b> send mail using your <b>unsecured</b> mailbox. If you have payments to send, mail them at your local post office.	
<b>Never</b> print your Social Security Number on your checks.	
Keep items that contain your <b>personal information in a safe place</b> .	
Don't give out personal information on the phone or in person unless you know <b>exactly</b> whom you are dealing with.	
Don't give your SSN unless it's absolutely necessary. Always show reluctance and ask for a randomly generated number for identification.	

<b>Action Item</b>	<b>Check</b>
<b>Computer Safety and Protection</b>	
Always use <b>an anti-virus</b> program. Update the data file regularly. I recommend automatic updates that run daily.	
Use a firewall to isolate your computer from the Internet and protect you from hackers.	
Use an anti-Spyware program. Update the data file for the program and scan your computer regularly. I recommend weekly scans.	
Never, ever open messages sent to you by anyone you don't know.	
Scams abound on the Internet and through e-mail. Don't fall for the tricks.	
Never, ever download files sent to you by anyone you don't know.	
Keep your computer operating system (Windows) up to date by downloading Windows Update from Microsoft's website. These updates are critical.	
Avoid keeping personal or financial information stored in your laptop computer. If you must carry that information, use a strong encryption program to protect these files.	
Enable the password on your laptop. That's the password needed to start the computer, not the Windows password.	
Use the latest Windows available (Windows XP) and set a strong password.	



## **Warning Signs of Identity Theft**

Warning signs include:

- You receive bills from a credit account you did not open.
- You see unauthorized charges on your credit, long distance, or bank accounts.
- You are contacted by a collection agency regarding a debt you did not incur.
- Checks disappear from your checkbook.
- Bank and credit billing statements don't arrive on time.
- Your credit report shows accounts you did not authorize.
- You are turned down for a credit card, loan, mortgage, or other form of credit due to unauthorized debts on your credit report.

## What to do if it happens to you

You have two options. Which one would you chose?

### Option 1

- Call your bank and/or Credit Card Company?
- Contact the three major credit repositories?
- Go through the helpful but expensive steps recommended by the Federal Trade Commission in its 30-page consumer support publication?
- Fill out and submit the affidavit form supplied by the FTC to dispute new, unauthorized accounts?
- Spend on average \$1,500 in out-of-pocket expenses and an average of 175 hours in your efforts to resolve the many problems caused by identity thieves?

### Option 2

#### **With the Identity Theft Shield™:**

Get regular monitoring of your credit report and let the proven leaders in the identity restoration and legal services fields assist you.

Isn't \$1 a day for protection worth the investment?

**Sign up for Identity Theft Shield™**