Surviving Identity Theft

by Mike Payne

SOMEBODY YOU KNOW AND LOVE WILL

"RUN IN TO" THIS FACELESS, NAMELESS "ATTACKER" AND…

…YOUR LOVED ONE'S LIFE WILL NEVER BE THE SAME!

"My life…my family's lives…changed overnight. We will NEVER recover…we will NEVER get back what was stolen from us. We had no idea just how bad this attacker could be…we had no idea!"

It was a call Karen Myers never expected. It was a phone call that would forever change her life. On the phone was a fraud investigator, and she wanted to know if Myers had recently established an account with Wachovia Bank.

"Ma'am, I have never even heard of Wachovia," said Myers, 39, a school teacher outside of Wichita, Kansas. "That's what I thought," the investigator replied.

Someone had tried to open a Wachovia credit account using Myers's social security number and name, but a different date of birth. Myers learned about it in October, 2006.

The call was the beginning of two frenzied months in Myer's life, months that transformed her from a small-town nurse into a private investigator and an identity theft expert. Her aggressive efforts to salvage her credit and good name cost Myers entire weeks of her time and upended her life.

FACT This is a national epidemic. Approximately 15 million Americans fall victim to identity theft each year.

**FACT ** Victims of identity theft spend an average of $1,400 in out-of-pocket expenses to resolve problems created from this crime.

Eventually those efforts led to a dramatic arrest in suburban Phoenix, Arizona., just as the thief was attempting her biggest scam yet. Myers's story proves that sometimes the best way to stop an identity thief is to take matters into your own hands.

Can Of Worms Opened

When she discovered she had become a victim of identity theft, Myers called the Experian credit bureau and placed a fraud alert on her credit report. In the process, she discovered that the thief had opened two Sears credit cards and two Chase credit accounts in her name.

FACT Contact all 3 Credit Bureaus by phone to have your records fraud flagged with a 7-year flag. Alert them that your identity has been stolen. Tell them you will back it with written proof (the police report), and ask them to what address to send the proof. THIS IS A FREE SERVICE on the part of the Credit Bureaus and it's the law.

- Equifax - Fraud Dept. Number: 1_800_290_8749
- Trans Union - Fraud Dept. Number: 1_800_680_7289
- Experian - Fraud Dept. Number: 1_800_583_4080

Like most synthetic identity thieves, the scammer blended different bits of Myers's personal data with information gleaned from other sources, including some information from the thief's own life.

The common denominator to all the accounts was Myers's Social Security number. Given the patchwork nature of a synthetic identity, it can take years to unravel the tangled mess of this type of crime.

Often, because the name does not match the Social Security number, the crime won't always show up on legitimate credit reports. If victims ever actually discover the crime, clearing one's name can be much more complicated than it would have been in the case of true-name identity theft.

MYERS HAD HER WORK CUT OUT FOR HER; LUCKILY, SHE WAS UP TO THE TASK. MYERS TOLD EXPERIAN THAT THE SEARS AND CHASE CARDS WERE NOT HERS.

The accounts were expunged from her credit report.

Many people would have stopped there, but Myers kept digging. She called Visa, MasterCard and Fashion Boutique and ordered all new credit cards.

Then she called Target's department store, where she had an account.

Wait a minute, said the woman in the store's corporate credit office.

Hadn't Myers walked into a Target store in Arizona just the night before and bought $932.89 worth of clothes and shoes?

No, Myers said through gritted teeth. She had been sleeping in her bed, 1,200 miles away.

FACT Family members, friends, employees at stores at which you shop, co-workers and others known to the victim commit a mojority of ID theft crimes.

However, that's quickly changing as technology makes it 'easier' for thieves to steal our precious personal information.

The thief didn't even have a Target credit card.

The store allowed her to make the purchase using Myers's account number, plus a fake ID with Myers's name and Social Security number. "I thought that was bogus as heck," Myers says. "Why do they set up the computer system and ask for an address and driver's license if they don't even check it?"

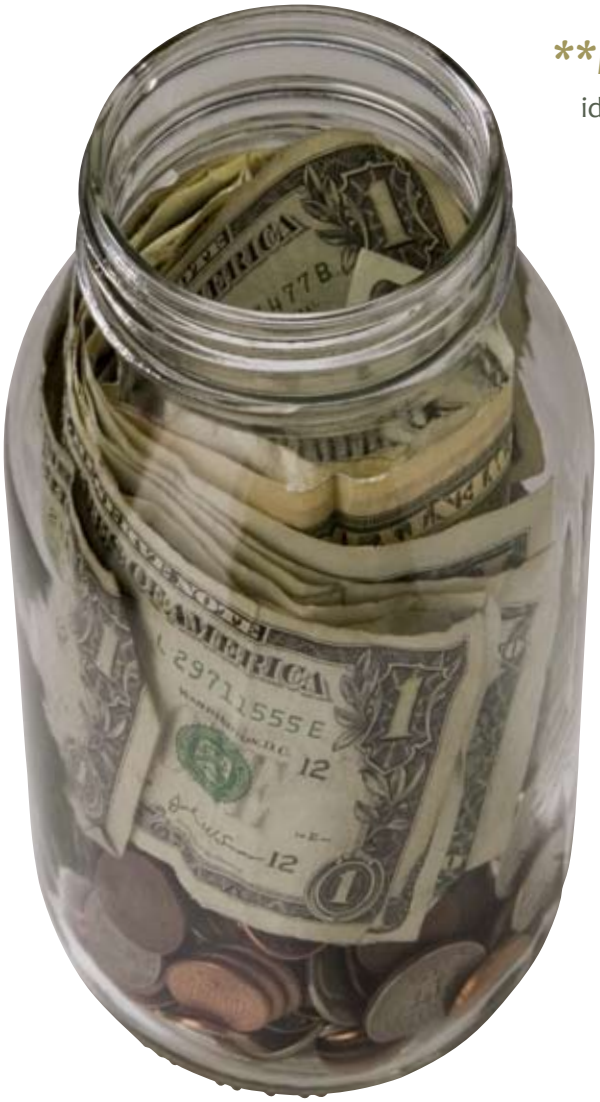
Fortunately, Target gave Myers her first solid lead. The thief had placed her real address on the fake ID: Northumbria Drive, near Mesa's south side.

Myers's next big break, and her biggest hassle, came when she checked her credit report and discovered someone had bought five Verizon cell phones and a Direct TV account using Myers's Social Security number.

In a conversation with Verizon, Karen Myers pried loose the name her suspected identity thief had used to open the cell phone accounts: Shaneeka Adkins. "It's really amazing how much information you can get from people when you're friendly," says Myers.

Alone among all the companies she dealt with, Direct TV refused to expunge Karen Myers's credit, insisting she was responsible for months of service.

When Myers refused to pay, the company sent her account to a collections agency. It was only when Myers requested the intervention of the Kansas State Attorney General that Direct TV relented. But whoever was using her identity proved even harder to deter.



FACT If you discover that you are a victim of identity theft you should report the incident to the police deparment in the city or town where you live. Make sure you get a copy of the police report, and keep a record of the officer's name and contact number.

The FTC provides an ID Theft Affidavit that can help you organize and accurately record your complaint. All three major credit bureaus and most of the large lenders accept this form as notice from you. You can also call the ID Theft Clearinghouse toll-free at (877) ID-THEFT (438-4338) to report the theft. If the crime involves your Social Security number, call (800) 269-0271 or visit the Social Security Administration's website.

The suspect ordered a VISA card and obtained a Shell gas card in Karen's name, while somehow managing to charge $10,000 worth of gas in two weeks. "She really went to town," Myers says.

ONE STEP AHEAD Myers reacted by closing all her credit, savings and checking accounts, and creating new ones. It was lucky timing. The day after Karen closed her checking account, Shaneeka attempted to use it five separate times to make PayPal purchases online.

Eleven days later, Karen discovered something even more shocking: Somebody had filed a change of address form with the U.S. post office, diverting all of Karen's mail, including her brand-new credit cards, to a post office in Arizona. "I was like, 'Oh shoot,'" Myers says.

Myers called the U.S. Postal Inspector's office and told her story. The inspector obtained a warrant to search the box and keep it under surveillance.

But she didn't stop there—she was worried that her nemesis might also try to steal the identity of her husband, Robert.

So, on a Saturday morning, Robert Myers called the three credit bureaus and requested a fraud alert on his credit report. Turns out that their fears were not unfounded.

FACT Contact all 3 Credit Bureaus by phone to have your records fraud flagged with a 7-year flag. Alert them that your identity has been stolen. Tell them you will back it with written proof (the police report), and ask them to what address to send the proof. THIS IS A FREE SERVICE on the part of the Credit Bureaus and it's the law.

- Equifax - Fraud Dept. Number: 1_800_290_8749
- Trans Union - Fraud Dept. Number: 1_800_680_7289
- Experian - Fraud Dept. Number: 1_800_583_4080

That very night, the Myerses received a phone call from a car dealer in Chandler, Arizona. A man and woman had walked into the dealership and asked to buy two cars, together worth over $82,000.

The man was using the name Robert Myers.

But when the dealer ran the man's credit, he discovered the recently-placed fraud alert. Is the real Robert Myers sitting in my dealership, the dealer asked. No, Robert replied. He was home in Kansas.

The salesman hung up, phoned the police and returned to the showroom, where he distracted the couple, keeping them occupied until the police arrived.

Shaneeka Ulinda Myers and her male accomplice were arrested.

Adkins was charged with placing fraudulent credit applications and fraudulent use of identification documents, both felonies.

A HARD-WON VICTORY... ALMOST...

As Karen Myers found, identity thieves can be relentless (and shameless) when it comes to exploiting your identity, and defending yourself against their tactics can become a full-time job.

**FACT ** Victims of identity theft lose an average of $16,000 in wages in their efforts to resolve the consequences of the theft, according ot the Identity Theft Resource Center.

"I do thank God that I was always able to stay a step ahead of her"

FACT Victims now spend an average of 600 hours recovering from identity theft.

What saved Karen Myers from extensive financial ruin was her unyielding attention to her credit file and accounts and her willingness and ability to do the legwork.

Though graced with good timing in some instances, she prevailed ultimately because she was well informed about the available tools with which she could defend herself—and she wasn't afraid to use them.

FACT Most identity theft goes unnoticed until the thief has caused extensive, irreparable damage...often too late for an effective police invesigation.

By placing a fraud alert on her credit file and following up with each questionable charge, Myers proved that it's possible to block most abuses. "I do thank God that I was always able to stay a step ahead of her," she says.

Shaneeka Myers's trial is scheduled to start Oct. 1, and her problems have compounded since her arrest.

On October 21, Shaneeka posted her $5,000 bond with the A + Bail Bonds company. The credit card she used was fraudulent. It had Karen Myers's name printed on the front. Consumers Union estimates an average of 27,000 Americans become victims of identity theft each day.

Cyveillance, a security firm that crawls the Internet looking for tainted websites, has found more than 1 million stolen Social Security numbers on computer servers controlled by criminals.

Only 22% of victims had a clue how they were victims of identity theft.

****Scary Reality #1**** 40 percent of Americans, under the age of 25, believe they are more likely to be hit by lightning, to be audited by the IRS, or to win the lottery than be the victim of a computer security problem --The National Cyber Security Alliance (NCSA), 2004.

In truth, Internet-related threats, including viruses, phishing scams, and hacking, affect about 70 percent of computer users! While the odds of being hit by lightning are 0.0000102 percent, according to the U.S. National Weather Service. - BBC, 2004

I didn't know what had hit me or to what extent. I too was a lucky one. It could have been worse...I think."

- And this is an OLD 2004 survey! We can only hope the 25 and under age groups see this more seriously today. Identity theft will INCREASE, not decrease in time as more thieves realize the ease (and understand the tools) of hitting computer keys opposed to sifting through the private information you inadvertantly toss into the garbage.

****Scary Reality #2**** Our random survey recently returned the following surprising result – a majority of respondents stated that because they are not personally responsible for any money spent on purchases by a thief who stole their identity, there's little if any concern! Can people really be this uninformed about the seriousness of ID Theft?

- Apparently, those people don't understand the emotional turmoil, money and time involved in fighting ID Theft.
- Karen and Robert Myers are the lucky ones. They knew enough to pursue ID thief Shaneeka Adkins and basically hand her to the police. Karen Myers is the exception, not the norm.
- Most people do not regularly pull and review their credit reports.
- Most people would not know what hit them and they wouldn't know where to begin. That's typical. That's what happened to me back in 1984. I didn't know what had hit me or to what extent. I too was a lucky one. It could have been worse… I think.

As victims deal with the aftermath of this crime, life will not return to normal -- in too many cases, victims do not get the help and understanding they deserve, 'discredited' by many creditors, potential creditors or perhaps employers and landlords.

HARD TO BELIEVE?

That's what we thought too. The reality is that not everybody is sensitive to or understanding of identity theft.

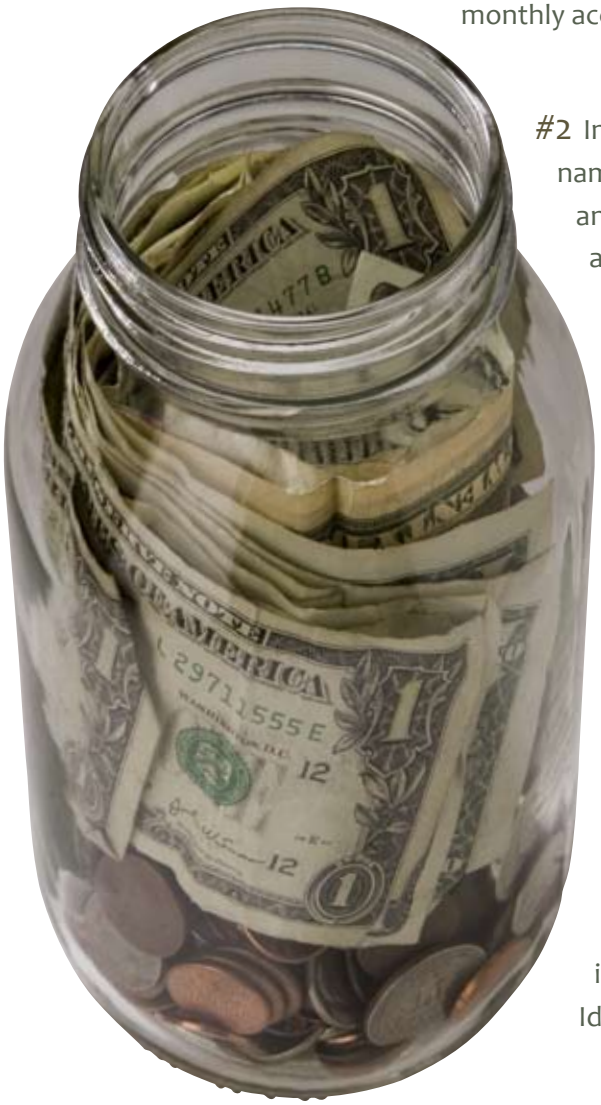
Victims will have problems getting new credit, procuring personal loans, renting an apartment, and even getting hired.

Victims of identity theft often find that the authorities are overwhelmed and unable to render tangible assistance, as victims try to confront Identity Theft.

What Is Identity Theft?

There are two primary types of crime related to identity theft:

#1 Account takeover occurs when a thief acquires a person's existing credit account information and uses the existing account to purchase products and services. Victims usually learn of account takeover when they receive their monthly account statement.



#2 In true identity theft or application fraud (often called true name fraud by experts), a thief uses another person's SSN and other identifying information to fraudulently open new accounts and obtain financial gain. Victims may be unaware of application fraud for an extended period of time — which can allow the thief to continue the ruse for months, even years.

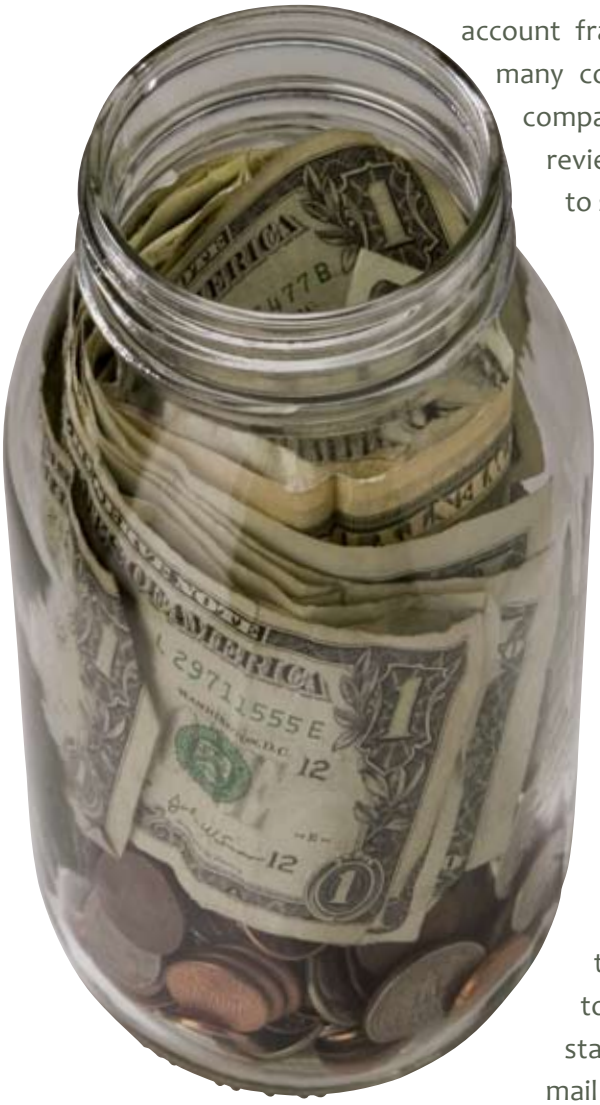
What Thieves Do and How You Can Stop Them!

Stealing wallets and purses was once the most common way of obtaining SSNs, driver's licenses, credit card numbers, and other identifying information. And these thefts continue today, moreso than ever before.

However, more readily available 'tools' and the potential reward lure identity thieves to attack virtually every area of your life — wherever you store or send personal information. Whether crime ring stealing and selling your Identity or individual stealing your purse, you will suffer.

THE ONLY UNANSWERED QUESTION IS TO WHAT EXTENT WILL YOU SUFFER? AMONG IDENTITY THIEVES CURRENTLY FAVORED METHODS INCLUDE:

CheckBook and/or Checking Account Theft – Checking Account Theft of Identity. The most hard-to-resolve issues for victims of theft of identity happen when the thief is able to obtain a checking account in the identity of the victim. Checks written on this account fraudently opened in your name will now involve many collection agencies. For additional information on companies providing 'check guarantee' services, please review the following companies as check fraud occurs to some degree in most ID theft cases:



- CrossCheck: (800) 654_2365 or 707_586_0431
  www.cross-check.com
- Certigy: (800) 437_5120
  www.certegy.com
- SCAN: (800) 262_7771 or 1_877_382_7226
  www.scanassist.com
- TeleCheck: (800) 366_2425
  www.telecheck.com

Dumpster Diving—Identity thieves know what to look for in the trash. They sift through your garbage to find personal information such as bank and credit card statements. We toss credit card and loan application 'junk' mail into the trash cans without a second thought. It's so annoying. Into the trash goes our paper bank and credit card statements and receipts as well. We make it so easy for thieves to piece together enough information about our financial lives to haunt us for a lifetime.

*****TIP**** Place the shredder near where you open junk mail or pay the bills. Or place a special trashcan nearby and shred later – the trashcan is used only for sensitive 'shred later stuff'.

Mail Theft—Thieves look for anything in the mail that contains personal information such as financial account statements and bills and remove it before you even know it was sent to you. Mail thieves know when Payroll sends out 1099s for instance.

In one case, the thief had been taking mail out of the poorly secured boxes using a key fashioned out of a knife. She was able to come and go as she pleased and remove mail from the back of the mailboxes without anyone seeing. Many community 'group' mailboxes are poorly secured, making access to thieves relatively easy. She had timed the thefts toward the end of the month when paychecks and bills were most commonly received. And during the last 2 weeks of January she was hitting the jackpot on a daily basis by stealing W2s, 1099s and other tax-related documents.

- In the event of mail theft, Call the U.S. Post Office at 1_800_275_8777 to obtain your local postal inspector's contact information.
- Tell them that you suspect your mail has been stolen and ask them to check to see that no one has changed your address.
- Remove your name from mailing lists for pre-approved credit lines by calling 1_888_5-OPTOUT (1_888_567_8688).

Stealing—From having purse or wallet stolen to dishonest employees removing sensitive files from businesses that store your information. Salespeople and waiters have been known to memorize or copy your credit card numbers. In your Home—Friends, houseguests, maintenance workers, babysitters, and cleaners can steal or copy your sensitive information right from under your nose.

Contact all credit card issuers, flag all fraud accounts

*****TIP***** Clean out your wallet or purse, keeping only 'essential' credit card, driver's license, etc. On a piece of paper kept in a safe, accessible spot, make copies (front and back) of all important contents kept in your purse or wallet. In the event your purse or wallet is stolen, you can quickly contact all issuers.

- Contact your bank, fraud flag all accounts;
- Contact the Department of Motor Vehicles, fraud flag your driver's license;
- Contact the State Department and fraud flag your passport.

***Personal Computers and the Internet*—**Most ID theft still occurs the old-fashioned way with thieves rummaging through your trash, stealing your mail, copying your credit card info as you pay your restaurant or department store bill. However, 'eCrime' is growing and getting more sophisticated.

*****TIP***** By all means, protect your computers, starting with a software firewall. Though many IT people will say your router provides enough protection with its hardware firewall, we recommend a software firewall as well.

- Microsoft offers a free software firewall with XP and Vista (I don't know about earlier versions)
- Best 'PAID' firewall = Norton Internet Security 2008
- Review @ ***http://www.pcmag.com/article2%,1895,2180639,00.asp***

Viruses are a piece of programming code disguised as something else that causes an unexpected and usually undesirable event. It's often designed to be automatically spread to other computer users. Viruses can be transmitted as attachments to e-mails, as downloads or be present on a diskette or CD. The source of the infected e-mail, download, or diskette you've received is often an unwitting co-conspirator. Some wreak havoc as soon as their code is executed, while others lie dormant until circumstances cause their code to be executed by the computer.

*****TIP***** You MUST have anti-virus. Do not use a Windows computer on the Internet without AV software. Use your anti-virus software and keep your definitions file updated.

- Best 'PAID' anti-virus = Norton Internet Security 2008
- Review @ ***http://www.pcmag.com/article2%,1895,2180639,00.asp***
- Best 'FREE' anti-virus = AVGupdated.

Worms are a self-replicating virus that does not alter files but resides in computers' active memory and duplicates itself. It can arrive in the form of a joke program or software. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, which slows or halts regular computer tasks.

Trojan Horses are a program that neither replicates nor copies itself but contains apparently harmless data that can damage or compromise the security of your computer. Typically, a friend innocently forwards you a Trojan horse in the form of a joke program or type of software. Sophisticated viruses and worms often replicate themselves by mailing email messages, with a Trojan attached, from an already infected computer. These malicious programs find email addresses to send to by using the infected computer's address book. Novice web users are especially susceptible to these kinds of attacks, because they aren't likely to suspect attachments that are attached to emails from the computer of a friend which may be infected with the virus or worm.

- Best "PAID' anti-Trojan Horse = Norton Internet Security 2008
- Review @ ***http://www.pcmag.com/article2%,1895,2180639,00.asp***

Spyware is technology that aids in gathering information about a person or organization without their knowledge. On the Internet, it is put on someone's computer and relays information to advertisers or other interested parties. Most often, it hides behind other software as you download it. If you're a heavy user of post-Napster file-sharing programs like Morpheus, Limewire or Kazaa, both known distributors of spyware, you're probably already infected. Cookies, which generally are not bad, allow Internet site owners to personalize websites for users and to keep track of their identities when they log in but can also be used to track some web usage. Once on your PC, spyware can sequester itself deep inside your operating system in what is known as the registry files. Anti-virus software won't spot it because it looks like something you chose to install.

- Best 'FREE' anti-spy and adware = Ad-Aware
- Best "PAID' anti-spy and adware = Norton Internet Security 2008
- Review @ ***http://www.pcmag.com/article2%,1895,2180639,00.asp***

Adware refers to any software application in which advertising banners are displayed while the program is running. It often includes spyware code that tracks your personal information and passes it on to third parties.

- Best 'FREE' anti-spy and adware = Ad-Aware
- Best "PAID' anti-spy and adware = Norton Internet Security 2008
- Review @ ***http://www.pcmag.com/article2%,1895,2180639,00.asp***

Phishing is a form of identity theft that uses e-mails and fraudulent web sites designed to fool you into giving away your personal information such as home address, account numbers, or usernames and passwords.

*****TIP***** Do not respond to all the 'official-looking' emails slamming our email Inbox appearing to come from a (your) bank, a Nigerian diplomat wanting to give you money as a reward for helping him, eBay, PayPal, etc.

- That 'junk' mail is trying to get you to give out personal information. Do not click a link and/or give out any personal information. At the very least, call the bank if you think the email is legitimate.

    - ID thieves play numbers. They know that sex sells and that they can promise you a photo of some nude girl or guy if you click on the blue link. Don't click on the enticing spam emails filling your Inbox daily. Please train your children, as their innocent actions could infect your home network of computers or even one computer.

    - Best 'PAID' spam filter = Norton Internet Security 2008

    - Review @ ***http://www.pcmag.com/article2%,1895,2180639,00.asp***

Scam Artists—Thieves often imitate someone who would request personal information such as a telemarketer, a representative from your employer or bank, a member of a law enforcement agency etc. These 'smooth-talking' thieves often make us wonder how they ever got us to trust them enough to let them in our house to use the telephone, go to the bathroom or get personal information over the phone.

PC Repair People – Julie S. of Orlando, FL, took her 'broken' computer to a computer repair shop referred to her by a good friend. A week later, Julie complained to her brother, who was visiting from out-of-state and an IT person, that her computer still was giving her lots of problems. It was slow and 'erratic.' Her brother Sean ran many diagnostics programs. What he discovered actually shook him up.

Sean discovered a malicious 'keylogger' script loaded onto Julie's computer. A keylogger is a type of surveillance software (considered to be either software or spyware) that has the capability to record every keystroke you make to a log file, usually encrypted. A keylogger recorder can record instant messages, e-mail, and any information you type at any time using your keyboard. Keyloggers, as a surveillance tool, are often used by employers to ensure employees use work computers for business purposes only. Unfortunately, keyloggers can also be embedded in spyware allowing your information to be transmitted to an unknown third party. The log file created by the keylogger can then be sent to a specified receiver.

SOME KEYLOGGER PROGRAMS WILL ALSO RECORD ANY E-MAIL ADDRESSES YOU USE AND WEB SITE URLS YOU VISIT. RESULT:

- Julie's online-banking – potentially compromised!
- Julie's address book – potentially compromised!
- Julie's passwords for everything on- and offline – potentially compromised!
- Julie's entire computer – potentially compromised!

Most horrifying was Sean's last statement to Julie still sending chills down my spine: that keylogger program could allow a thief to control Julie's computer as if he was sitting at the keyboard; he also could control Julie's webcam ALL WITHOUT Julie even knowing it!!!!!!!!!!!!!!

WOW! This 'thief' could control Julie's webcam too! OMG!

The story doesn't end here. Wait until you hear what Sean and Julie did next. Even George Orwell couldn't have imagined this.

How Can You Reduce The Risk Of Identity Theft?

Unfortunately, established personal habits and lax credit industry practices make it relatively easy for criminals to commit identity theft. Nonetheless, you can reduce your risk considerably. The three most important things you can do are:

- Scrutinize your credit report at least twice a year.
- Sign up for a credit monitoring service.
- Periodically check other personal records, such as your DMV file.

That said, every potential target of identity theft — and that means anyone with a credit card, a bank account, a driver's license, or a Social Security number — should minimize his or her risk by following the five steps described below:

1. Know your personal information — and your vulnerabilities
2. Reduce your exposure
3. Make your data useless to criminals
4. Review your information regularly
5. Act fast if trouble strikes.

For anyone who doesn't know you personally, face to face, your personal information is the key to proving that you really are who you say you are. This makes it immensely valuable — and not just to you.

What Is Worth MORE Than Gold To ID Thieves?

Here are the pieces of personally identifying data that identity thieves covet most:

- Your Social Security number (SSN)
- Your driver's license
- Your credit card information
- Your bank account information
- Your mother's maiden name
- Your home address and phone numbers
- Any other information that helps an imposter pretend to be you

Your Social Security number, in particular, is the key to your credit card and bank accounts and, therefore, a prime target for criminals.

TIP Release your SSN only when absolutely necessary — for tax forms, employment records, bank statements, stock and property transactions, and so on.

TIP Do not carry your Social Security card in your wallet except in situations where it's truly required, such as your first day on a new job.

TIP Avoid carrying wallet cards that display your SSN — health insurance cards being the most notable example — except when necessary to receive care.

TIP Avoid providing your SSN on job applications if at all possible.

TIP Don't have your SSN (or your driver's license number, for that matter) printed on your checks.

****TIP**** Don't allow merchants to add your SSN to your checks by hand. (There's no law against this, so you may need to be assertive.) If a business requests your SSN, ask if there's an alternative number that can be used instead. Speak to a manager or supervisor if your request is not honored, and ask to see the company's written policy on SSNs. If necessary, take your business elsewhere.

"If you are hit by identity theft, time is of the essence!"

If a government agency requests your SSN, look for a Privacy Act notice. This will tell you if your SSN is required, what will be done with it, and what happens if you refuse to provide it.

In the wrong hands, your home address can create two specific vulnerabilities: mail theft and burglaries that target your personal information. As for your mother's maiden name, people still accept it as proof of identity, so do your best to protect it. Never use it as a password yourself.

Use credit monitoring to alert you to suspicious credit activity and possible fraud. Each month, carefully review your credit card, bank statements, and phone bills (including mobile phones) for unauthorized use.

****TIP**** Take a look at ***www.truecredit.com*** for what we feel is the most comprehensive and economical credit-monitoring choice.

Examine your Social Security Personal Earnings and Benefits Estimate Statement each year to check for fraud. The Social Security Administration mails this statement to adult SSN holders about three months before their birthdays.

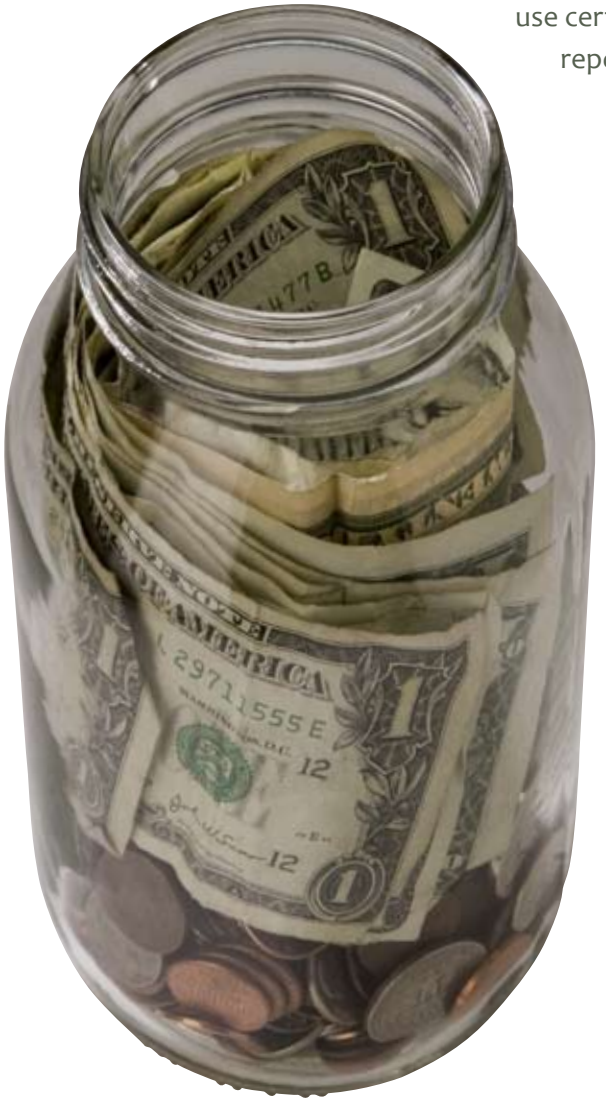
If you are hit by identity theft, time is of the essence.

With hope, you will read this report (a few times) and then do what the report suggests while you still can.

Then, if/when you are hit, you will know what to do and how to do it without losing your head.

Assess the situation — but do it quickly, preferably with the guidance of someone who knows this complex terrain and is committed to seeing you through the whole process. Then determine what needs to be done and begin reclaiming your identity.

TIP Get Your Reports Immediately! Each credit bureau will mail you a free credit report once you've called in a fraud alert. These alerts are usually placed for 90 to 180 days, but may be extended. Do so in writing, following the directions sent in the credit report you receive. You may cancel fraud alerts at any time. In all communications with the credit bureaus, you'll want to refer to the unique number assigned to your credit report; here again, use certified return receipt mail. Be sure to save all credit reports as part of your fraud documentation.



- Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been opened, if this information isn't already included on the credit report.

- Ask the credit bureaus in writing to remove inquiries generated due to the fraudulent access.

- You may also ask the credit bureaus to notify those who have received your credit report in the last six months (two years for employers), alerting them to the disputed and erroneous information.

- Be aware that these measures won't necessarily prevent new fraudulent accounts from being opened by the imposter, since credit issuers are not required by law to observe fraud alerts.

- Request a free copy of your credit report every few months so you can monitor for fraud.

****TIP**** Immediately contact all creditors with whom your name has been used fraudulently, by phone and in writing. You'll see evidence of these accounts on your credit reports.

- Complete Fraud Affidavit and Police Report. Creditors will likely ask you to fill out fraud affidavits. The Federal Trade Commission provides a uniform affidavit form that most creditors accept. No state or federal law requires affidavits to be notarized at your own expense; you may choose to substitute witness signatures for notarization if creditors require verification of your signature.

- Ask the credit grantors to provide you and your investigating law enforcement agency with copies of the documentation, including the application and records showing the fraudulent transactions.

- Get replacement cards with new account numbers if your existing credit accounts have been used fraudulently,. Ask that old accounts be processed as "account closed at consumer's request" (better than "card lost or stolen" because it can be interpreted as you

- taking the blame.) Monitor your mail and bills for evidence of new fraud; report anything you find to creditor grantors immediately. Add passwords to all accounts; avoid your mother's maiden name or any easily guessed word.

- Correct ALL Debt collectors. If debt collectors try to make you pay the unpaid bills on fraudulent credit accounts, ask for the company name, the name of the person contacting you, and the phone number and address.

- Tell the collector you are a victim of fraud and are not responsible for the account.

- Ask for the name and contact information for the referring credit issuer, the amount of the debt, the account number, and dates of the charges.

- Ask if they need you to complete their fraud affidavit form or if you can use the Federal Trade Commission form.

- Follow up in writing to the debt collector, explaining your situation.

- Ask that they confirm in writing that you do not owe the debt and that the account has been closed.

TIP Get Police Report. This is something you do not want to hear. It's better you hear it now, BEFORE you suffer an ID Theft nightmare. Some police departments may be reluctant to file reports on 'alleged' ID crimes – be persistent.

TIP Get Legal Help. You may wish to consult an attorney to determine legal action against creditors and/or credit bureaus if they aren't cooperative in removing fraudulent entries from your credit report or if negligence is a factor.

Call your local Bar Association, Better Business Bureau, or Legal Aid office to find an attorney specializing in consumer law, the Fair Credit Reporting Act, and the Fair Credit Billing Act.

NOTE** Go to ***www.naca.net for a consumer attorney near you. They are GREAT, though I hope you never will need to contact them.

If you're a senior or care for a dependent adult, look for referral centers under Elder Law or Aging and Independent Services.

TIP Lost or Stolen ATM card. Banks contribute to lost ATM cards. Many ATMs today suck your card into the machine, allowing you to walk away with your card still inside the machine. Get with it, Banks. Read the magnetic strip without sucking our cards into the ATM. Eliminate lost cards happening this way.

My corporate friend inside Bank of America tells me this is so incredible and prevalent that he too cannot believe BofA and others have not changed the way ATMs take your card. Was your ATM or debit card stolen or compromised?

- Report it immediately.
- Get a new card, account number, and password. Do not use your old password. When creating a new one, don't use easy-to-guess numbers, like the last four digits of your SSN or your birthdate.
- Monitor your account statement. You may be liable if fraud is not reported quickly.
- Be sure to read the debit card contract for liability; some cards are better protected in cases of fraud than others.

Many people are surprised by the emotions they experience after suffering identity theft, account takeover, or some other event that puts their identity at risk. Your urgent need to take some kind of action may be undercut by feelings of frustration, helplessness, and confusion. Your desire to know how this happened and how it will end may feel blocked by a brick wall of uncertainty.

The most practical, capable, and optimistic people may feel depressed and unable to focus, while people who are normally stable and even-tempered may find their emotions in a state of flux. And despite the support that family, friends, and colleagues may offer, many identity theft victims can't help feeling vulnerable and alone.

Naïve or Stupid? Only The Pain Mattered…

Back in 1984 while at college in Nebraska, I had a run-in with Identity Theft…I'll never forget it. On a warm, sunny Fall day, a bunch of friends and I met at a local park for some pick up basketball. In those days, we didn't think to roll up our car's windows or even lock the car's doors. How little did I know then just how painful my naive or stupid mistake would be.

In plain sight on the console between the front bucket seats, I left my wallet. Yes, I really did. After a few hours of ball, my friend Kevin and I hit the road to a nearby Taco Johns. It wasn't until we got to Taco Johns and I tried to pay that I realized I didn't have my wallet. No problem, I remembered, I had left it in the car. A few minutes later, I was panicking. I couldn't find my wallet anywhere. I tore my car apart.

It wasn't there. It was not anywhere. Kevin and I rushed back to the park and starting searching everywhere. A terrible feeling overwhelmed me. I hadn't experienced anything like this before. My head was spinning. My money…my driver's license…my credit card…my college ID (and in those days, the college used our Social Security number as our student ID). I didn't know what else I had in my wallet. I had no clue about Identity Theft. I didn't know where to begin. I did not want to believe somebody had stolen my wallet…***I did not want to believe somebody had gone into my car to steal my wallet.***

That was my first terrifying and painful introduction to Identity Theft. That event trashed my credit. I eventually filed a police report, but not until bank and credit card accounts were opened in my name….$1,000's of dollars in fraudulent purchases….many humiliating and angry debt collection calls later…so much wasted time and money defending my innocence…the bastards.

My life suffered for what seemed like an eternity. I made a huge mistake…I left my wallet out in plain sight in an unlocked car. Stupid…really stupid. I paid dearly for that mistake.

What scares me today, as I try to stay up on this stuff, is that I know what I know about Identity Theft. And what I know terrifies me. Each day, these thieves are getting more brazen and dangerous.

Somebody you know will get hit! Do not choose to become a victim. Do not choose to stick your head in the sand, believing this crime only happens to other people. Chances are, somebody you know and love will face this nameless, faceless attacker and your loved one's life will never be the same.

Please be safe. ID Theft does not have to happen to you or your loved ones.

~Mike Payne

"Take Action Now!"