

Identity Theft is a Major Problem in America

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

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

Experts recommend that you review your credit report regularly. The Identity theft shield makes it easy.

What if You Discovered That Your Identity Had Been Stolen?

1. Call your bank and/or credit card company
2. Contact the three major credit repositories
3. Go through the helpful but extensive steps recommended by the Federal Trade Commission in its 30-page consumer support publication
4. Fill out and submit the affidavit form supplied by the FTC to dispute new, unauthorized accounts
5. Spend on average \$1,500 in out-of-pocket expenses in your efforts to resolve the many problems caused by identity thieves

Or, with the Identity Theft Coverage:

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

The experienced leaders in the field...on your side who's that?

Kroll Background America

With the Identity Theft Shield™ you're backed by experienced professionals from a division of the world's leading risk consulting company.

And

Pre-Paid Legal Services ® , Inc.

With more than 30 years of providing legal rights protection to over 1.4 million families, PPLSI is a pioneer of the prepaid legal concept in North America.

What Does the Identity Theft Shield™ Cover?

Credit Reports

Evaluate your current credit standing with:

1. An up-to-date credit report through Experian at no added cost
2. A personal credit score calculated by an independent scoring service
3. A detailed analysis of your personal credit score

Experts recommend that you review your credit report regularly. The Identity Theft Shield™ makes it easy.

Continuous Credit Monitoring

Suspicious activation will be brought to your attention, providing you with early detection. You'll receive prompt notice if the credit repository is notified by Experian that:

1. New accounts have been opened in your name
2. Derogatory notations have been added to your credit report
3. Public records have been added to your report
4. Inquiries have been made against your report
5. A change of address has been requested

Identity Restoration

Identity theft can be devastating, and the process of restoring your name can be overwhelming and costly. You need more than "do it yourself" information if it happens to you.

With Identity Theft Shield™ a trained expert will take the steps to restore your name and credit for you!

- Help reduce your out of pocket expenses and time spent away from work with valuable services from detection to resolution.
- Fraud alert notifications will be sent on your behalf and applicable follow up will be done with affected agencies and institutions, including: credit card companies, financial institutions, all three credit repositories, Social Security Administration, Federal Trade Commission, Department of Motor Vehicles, law enforcement personnel, and the U.S. Postal Service.
- Proactive searches of applicable local and national databases will be made on your behalf to look for information you may not be aware of, including: criminal activity in your name in your county's records and certain federal watch lists, Department of Motor Vehicle records in your state, unknown addresses affiliated with your name, and banking activity in your name reported as fraudulent.

To know more about this service visit our web site at www.caases.org and click the ID Theft link.

(Id Theft) In Case Someone Steals or Uses Your Identity

ATTORNEY'S ADVICE -- NO CHARGE

Read this and make a copy for your files in case you need to refer to it someday. Maybe we should all take some of his advice! A corporate attorney sent the following out to the employees in his company.

- 1) The next time you order checks have only your initials (**instead of first name and last name put on them**). If someone takes your checkbook, they will not know if you sign your checks with just your initials or your first name, but your bank will know how you sign your checks.
- 2) Do not sign the back of your credit cards. Instead, put "**PHOTO ID REQUIRED**".

3) When you are writing checks to pay on your credit card accounts, DO NOT put the complete account number on the "For" line. Instead, just put the last four numbers. The credit card company knows the rest of the number, and anyone who might be handling your check as it passes through all the check processing channels won't have access to it.

4) Put your work phone # on your checks instead of your home phone. If you have a PO Box use that instead of your home address. If you do not have a PO Box, use your work address. Never have your SS# printed on your checks. (DUH!) You can add it if it is necessary. But if you have it printed, anyone can get it.

5) Place the contents of your wallet on a photocopy machine. Do both sides of each license, credit card, etc. You will know what you had in your wallet and all of the account numbers and phone numbers to call and cancel. Keep the photocopy in a safe place. I also carry a photocopy of my passport when I travel either here or abroad. We've all heard horror stories about fraud that's committed on us in stealing a name, address, Social Security number, credit cards. Unfortunately, I, an attorney, have firsthand knowledge because my wallet was stolen last month. Within a week, the thief(s) ordered an expensive monthly cell phone package, applied for a VISA credit card, had a credit line approved to buy a Gateway computer, received a PIN number from DMV to change my driving record information online, and more. But here's some critical information to limit the damage in case this happens to you or someone you know.

Footnote: Get an Id Theft & Prepaid legal plan that will give you a monthly report if you have had activity on you credit or not plus one that will give you unlimited talk time. Plus one that will give you contract / document review and a "Will". This will help you save \$100's to \$1000's a year.

6) We have been told we should cancel our credit cards immediately. But the key is having the toll free numbers and your card numbers handy so you know whom to call. Keep those where you can find them.

7) File a police report immediately in the jurisdiction where your credit cards, etc., were stolen. This proves to credit providers you were diligent, and this is a first step toward an investigation (if there ever is one).

But here's what is perhaps most important of all:

(I never even thought to do this.)

8) Call the 3 national credit reporting organizations immediately to place a "**fraud alert**" on your name and Social Security number. I had never heard of doing that until advised by a bank that called to tell me an application for credit was made over the Internet in my name. The alert means any company that checks your credit knows your information was stolen, and they have to contact you by phone to authorize new credit. By the time I was advised to do this, almost two weeks after the theft, all the damage had been done. There are records of all the credit checks initiated by the thieves' purchases, none of which I knew about before placing the alert. Since then, no additional damage has been done, and the thieves threw my wallet away this weekend (someone turned it in). It seems to have stopped them dead in their tracks.

Again we repeat: Get an Id Theft & Prepaid legal plan that will give you a monthly report if you have had activity on your credit or not, one that will give you unlimited talk time, plus one that will give you contract / document review and a "Will". This will help you save \$100's to \$1000's a year.

Why wait to take these steps later when 75% of if it could be done for you now.

You do not need to pay more then \$39.00 a month for an ID Theft & Prepaid Legal Plan.

Get one now! Visit www.caases.org
Or call 1-888-439-3905

Now, here are the numbers you always need to contact if your ID has been stolen:

- 1.) Equifax: 1-800-525-6285
- 2.) Experian (formerly TRW): 1-888-397-3742
- 3.) Trans Union: 1-800-680-7289
- 4.) Social Security Administration (fraud line): 1-800-269-0271

5 Steps to Protect Your Identity

1. Protect Your Personal Information

- Your SSN is the key to your credit card and bank accounts – provide it only when absolutely necessary – for tax forms, employment records, bank statements, and stock and property transactions. Don't have it printed on your checks and do not carry it in your wallet.
- Don't leave mail in your mailbox where it can be stolen and mail bills only in Postal Service drop boxes.
- Change passwords and PINs on a regular basis. Don't use the last 4 digits of your SSN, maiden name, middle name, birth date, pets name or anything else that can be easily guessed. Memorize all passwords and don't record them on anything you carry in your wallet or purse.
- Tell companies, especially banks and credit card companies, not to sell your name.
- When filling out warranty cards, subscription forms, prize-drawing cards and web-site registration forms, fill in only the "required" info.
- Don't give your credit card number out to ANYONE on the telephone especially unsolicited telemarketers.

2. Reduce Your Exposure

- Unless absolutely necessary, don't carry a Social Security card, birth certificate or extra credit cards with you.
- At work, store your wallet or purse in a safe place.
- Photocopy all the cards and identifying info in your wallet, especially when you travel. On the photocopy, record the account numbers, customer service phone numbers and expiration dates so you can call the companies if your cards are ever stolen. Keep the photocopy in a safe place.
- Never allow anyone to write your credit card number on your checks.
- When shopping or paying bills online, choose companies that provide secure transactions. Before giving a credit card number, check to be sure the company's web address begins with "https://" which identifies it as a SECURE site.
- Avoid opening spam and other email from unknown sources – it may contain viruses or other programs that will make your computer vulnerable to hackers.
- Update virus protection software regularly.
- Install a firewall on your home computer, especially if you connect to the internet through a DSL or cable modem.

- Write the three major credit bureaus and ask to "Opt Out" of the pre-approved credit lists they sell to companies. Call 1-888-567-8688. Since the "opt-out" option may expire after two years, remind yourself to do it again.
- Internet scammers looking for people's financial information have a new way to lure unsuspecting victims: They go "phishing." Phishing is a high-tech scam that uses spam or pop-up messages to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information. The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequence if you don't respond. The message directs you to a Web site that looks just like a legitimate organization's site, but it isn't. The purpose of the bogus site? To trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

3. Make Your Data Useless to Criminals

- Shred documents (e.g., credit card receipts, phone bills, bank statements, investment account reports) before you throw them out. Invest in a good crosscut shredder for home use. Never trash preapproved credit offers without shredding them or tearing them into small pieces first.
- Before disposing of a computer, remove data by using a strong "wipe" utility program. Do not rely on the "delete function" to remove files containing sensitive information.
- Don't store financial information on your computer unless necessary, especially on laptops which are stolen more often. Use a password to help protect against this.

4. Review Your Information Regularly

- Order your credit reports twice a year to check for errors and fraudulent use.
- Use credit monitoring to catch suspicious credit card activity.
- Use fraud monitoring to catch attempts to alter or acquire your identity data.
- Review your credit card statements, bank statements and phone bills (including mobile phones) for unauthorized use.
- Check your Social Security Statement each year for signs of fraud.

5. Act Fast if Trouble Strikes

- Time is of the essence. If you discover evidence of identity theft (e.g., purchases you didn't authorize) you need to act quickly to minimize the damage.

Important Numbers

Equifax

P.O. Box 105069, Atlanta, GA 30348
 Report fraud: Call (800) 525-6285 and write to address above
 Order credit report: (800) 685-1111
 TDD: (800) 255-0056
 Web: www.equifax.com

Experian (formerly TRW)

P.O. Box 9532, Allen, TX 75013
 Report fraud: Call (888) EXPERIAN (888-397-3742) and write to address above.
 Order credit report: (888) EXPERIAN
 TDD: Use relay to fraud number above
 Web: www.experian.com

TransUnion

P.O. Box 6790, Fullerton, CA 92834
 Report fraud: (800) 680-7289 and write to address above
 Order credit report: (800) 888-4213
 TDD: (877) 553-7803
 E-mail (fraud victims only): fvad@transunion.com
 Web: www.transunion.com

To opt out of pre-approved offers....

of credit for all three bureaus, call (888) 5OPTOUT (888-567-8688).
 You can also opt out online at www.optoutprescreen.com
 You may choose a two-year opt-out period or permanent opt-out status

Social Security Administration

Report fraudulent Social Security benefits:
 (800) 269-0271
 Web: www.ssa.gov/oig/public_fraud_reporting/index.htm
 Or write to:
 Social Security Administration, Office of the Inspector General
 P.O. Box 17768, Baltimore, MD 21235

U.S. State Department, Passport Services

U.S. Dept. of State, Passport Services
 Consular Lost/Stolen Passport Section
 1111 19th St., NW, Suite 500,
 Washington, DC 20036

To Remove Your Name from Mail and Phone Marketing Lists:*Direct Marketing Association*

Mail Preference Service, P.O. Box 643,
 Carmel, NY 10512
 Web: www.dmaconsumers.org
 Online opt-out program costs \$5.00
 It is free by mail

FTC's Telemarketing Do Not Call Registry

(888) 382-1222
 Online registration: www.donotcall.gov

See PRC Fact Sheets No. 4 & No. 5

...on reducing junk mail and telemarketing calls
 Web: www.privacyrights.org/fs/fs4-junk.htm
 and www.privacyrights.org/fs/fs5-tmkt.htm

To Report Fraudulent Use of Your Checks:

CheckRite	(800) 766-2748
Chexsystems	(800) 428-9623
CheckCenter / CrossCheck	(800) 843-0760
Certify / Equifax	(800) 437-5120
International Check Services	(800) 526-5380
SCAN	(800) 262-7771
TeleCheck	(800) 710-9898