

Act Fast If You Are a Victim of Identity Theft

1. Contact the fraud unit

of the three credit reporting bureaus (toll-free numbers below). Ask for a **fraud alert** to be placed on your file and confirm that no new credit be granted without your approval. You can also request an extended fraud alert, which lasts seven years. The fraud alert tells creditors you are a fraud victim and that they must contact you before opening new accounts or issuing new cards.

Equifax: 1-800-525-6285

Experian: 1-888-397-3742

TransUnion: 1-800-680-7289



2. Notify your creditors or financial institutions to **close accounts** that have been opened or used by identity thieves. When you open new accounts, create new passwords.

3. If your driver's license or other government ID has been stolen or fraudulently used, **contact the issuing agency** to cancel the ID and get a new one.

4. File a police report and make copies. Credit card companies, banks and others may require it as proof of identity theft.

5. Report the theft to the Federal Trade Commission's identity theft hotline at 1-877-438-4338. A counselor can advise you on how to deal with the theft.

6. Complete an ID Theft Affidavit. The affidavit makes it easier for you to dispute debts incurred by identity thieves. You can get a copy at www.consumer.gov/idtheft or by calling the FTC's hotline at 1-877-438-4338 or 1-866-653-4261 (TTY).

Tip: Keep all your documentation in one secure place. You may need it for several months or even years until your case is resolved.

More Tips to Help Fight Identity Theft

DEALING WITH COLLECTION AGENCIES

One of the most stressful aspects of identity theft is the demand from collection agencies for payment of debts you didn't create. **What to do:**

Step 1 Write a letter to each agency stating that you are a victim of identity theft.

Step 2 Provide the collection agency with the following information:

- Copy of your driver's license or other government photo ID issued before the identity theft
- Certified copy of the police report
- ID Theft Affidavit
- List of financial institutions, account numbers, check numbers, etc., that are affected by the identity theft
- Statement that you are disputing the debt due to identity theft

SHOPPING OR SURFING ON THE INTERNET

Buy only from established, trustworthy **online retailers**. If you are unfamiliar with the company, check with the Better Business Bureau (www.bbb.org). Secure sites that protect your information have addresses that begin with <https://> ("s" for secure — non-secure sites begin with <http://>) and a closed padlock symbol in your browser window.

If you **receive an e-mail** requesting personal information that looks like it's from a company you do business with, **do not respond**. Government agencies, banks and other reputable businesses will never ask for your personal information this way.

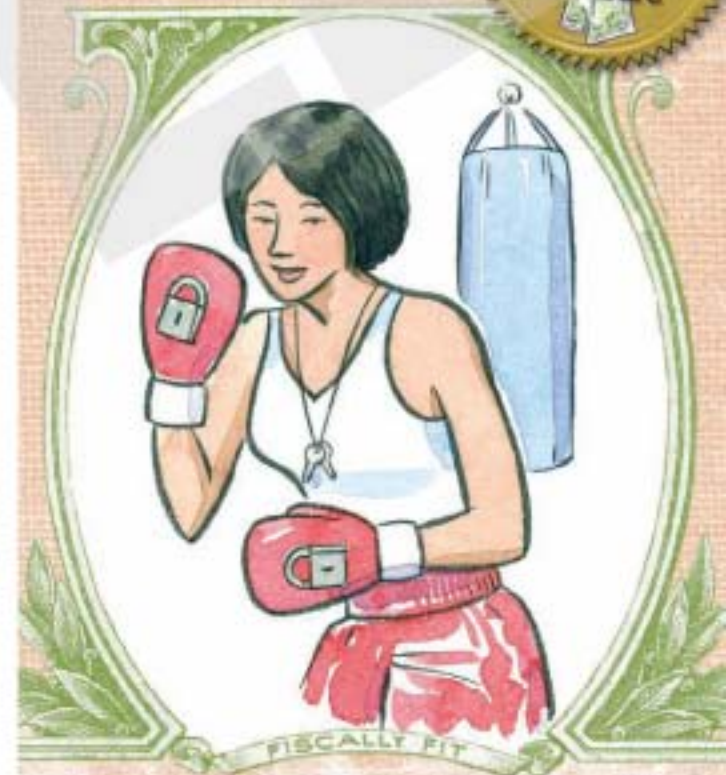
When shopping, **credit cards offer more protection** than debit cards. When you use a credit card, you can dispute fraudulent transactions before you have to pay for them.

Never send any personal information through e-mail.

This brochure is not intended as a substitute for professional services.
© 2007 Calstone Publishing, LLC, dba Personal Best.
A Highjas Cross Communication Company. All rights reserved.

PREVENTING IDENTITY THEFT

Smart Strategies and Self-Defense



PROTECT YOUR GOOD NAME

Are you a target for identity theft? Sad to say, many people are being hurt by the growing wave of crimes involving identity theft and fraud. Experts say a person could spend hundreds of hours cleaning up the financial mess left behind, often over a period of years. Are you doing everything you can do to avoid becoming a victim? This brochure offers tips and advice to help prevent identity theft — it's information every consumer needs.

How Does Identity Theft Happen?

It begins when personal information such as your name, birth date, Social Security number or credit card falls into the wrong hands — most often through:

- **Stolen** or lost purses, wallets, bank cards and checkbooks
- **Documents** found in residential and business trash
- **Stolen** paper or electronic records
- **Phishing** — e-mails requesting information about your bank account or other accounts (often using legitimate-looking logos and graphics of trusted banks and companies you may do business with)
- **Vishing** — a variation of phishing where you are instructed to phone in your sensitive information
- **Skimming** — when an ATM has been compromised to read your bank card number when you use your card

What's next? You have to clear your name, reestablish your credit, deal with collection agencies and cope with the stress of credit-related

problems caused by the theft. Use the checklist in this brochure to see how well you're guarding against identity theft.

Identity thieves typically use your name to...

open credit card, bank, Internet and other accounts — write bad checks

get a job, driver's license or government benefits — rent an apartment

obtain a loan — They may even use your name when they get arrested.

Strategies and Self-Defense for Identity Theft

ID Theft Prevention Primer: How well are you guarding your personal information? **Check each statement that applies:**

- I request a **free credit report** every 12 months from the three credit reporting bureaus at www.annualcreditreport.com or by calling 1-877-322-8228. Reviewing these reports is key to detecting fraud, according to the Better Business Bureau.
- I use **automatic** payroll **deposits** and online billing.
- I have **canceled credit cards** and other accounts that I no longer use.
- I visit my bank's and creditors' Web sites weekly to **monitor account activity**.
- I use a **crosscut shredder** to destroy private documents I no longer need.
- My Social Security number and driver's license number are not printed on my **checks**.
- I keep my Social Security number, bank cards and checks at home in a **secure place** unless I need them.
- I receive my **mail** at a P.O. box or a locked mailbox.
- I do not respond to **unsolicited e-mail** (spam) or to callers who ask for information such as Social Security and account numbers.
- I use **passwords** or codes that do not have obvious numerical sequences (e.g., 1234), my birth date, Social Security number or mother's maiden name.
- I do not store **confidential information** on computers, memory sticks, cell phones, PDAs or similar devices.
- I discard **electronic devices** and storage media (CDs, memory sticks) only after destroying all the data stored in them.
- I have asked my bank and credit card companies about their **anti-fraud programs** and their liability policy for fraudulent transactions.

Did you know? Consumers discover almost half of identity fraud cases, according to the Better Business Bureau. Be vigilant — take as many of the steps as possible listed above to protect yourself.



Don't Just Toss It — Shred It

Always shred documents that have your **personal information** on them. Use a crosscut shredder (one that cuts paper horizontally and vertically) to destroy unnecessary documents that contain any personal information, including:

- Account numbers
- Addresses
- Birth dates
- E-mail addresses
- Passwords and PINs for all family members, including children
- Phone numbers
- Signatures
- Social Security numbers (thieves will steal the Social Security numbers of babies)

Shred these documents when you no longer need them:

- Address labels from mail
- ATM receipts and bank statements
- Bills
- Birth certificate copies
- Canceled and voided checks
- Canceled credit and debit cards and associated paperwork
- Expired driver's license and employee, military or school IDs
- Expired passports and visas
- Junk mail containing personal information
- Legal, medical and insurance paperwork
- Luggage tags
- Pay stubs and other work records
- Presapproved credit applications
- Report cards
- Resumes
- Travel itineraries and used airline tickets
- Utility bills (phone, gas, Internet, water, cable TV)

