



What You Should Know About...

Identity Theft

- ▶ HOW IDENTITY THEFT HAPPENS
- ▶ PROTECTING YOURSELF
- ▶ RECOVERING FROM IDENTITY THEFT



You may have heard of a crime called identity theft, but you might not be sure exactly what it is, or how you can protect yourself against it. While identity theft occurs mostly on paper—someone uses your personal information to obtain credit in your name, mislead police, commit tax fraud, etc.—the impact it has on your financial life is very real.

There are a number of things you can do to protect yourself against identity theft. Understanding the value of your personal information, including your Social Security number and credit account information, is the first step in protecting yourself. And if, in spite of your best efforts, you have a problem with identity theft, there are steps you can take to repair the damage.

© 2005, HSBC Finance Corporation. All rights reserved.

This content is provided as educational material only and is not intended to solicit you for any product or service. These materials are not a recommendation by HSBC for any product, service or financial strategy. The suggestions and recommendations contained within are general in nature, and may or may not apply to your particular circumstances. Securities, annuity and insurance products are: not FDIC insured or insured by any federal government agency of the United States; subject to investment risk, including possible loss of principal invested. All decisions regarding the tax implications of your investment(s) should be made in connection with your independent tax advisor. Should you need further assistance, HSBC strongly recommends contacting an independent attorney, tax professional or financial consultant.

What is identity theft?

If someone steals your identity, you may not realize it has happened. But the effects can be serious. Identity theft occurs when your personal information, such as your name, account number or Social Security number (SSN) are used without your knowledge to commit fraud or theft. Armed with your personal information, thieves can make unauthorized purchases on your credit cards, apply for new credit cards and loans, cash bad checks, lease cars or mislead authorities, doing serious damage to your credit history.

Although you probably won't be held liable for fraudulent charges, clearing your name and credit history can be a time consuming, frustrating and lengthy process. In the most serious cases, it could take months or even years to complete, and during that time you might find it hard to get a loan, rent an apartment or even be hired for a job. As with many crimes, the impact can be emotional as well as financial.

There are two methods of identity theft:

1. The most common type of identity theft is someone using your stolen credit cards, debit



cards, checks or account information to make purchases or withdraw money from your accounts. You're likely to detect this type of theft when charges you haven't authorized show up on your credit card bill or when your bank or securities accounts are depleted.

2. Less frequently, but even more dangerous, someone might open new accounts in your name using your address, a stolen SSN or other forms of personal identification, and make purchases or obtain credit in your name. And if they use a different mailing address, you might not even learn the fraudulent accounts exist until you're turned down for credit or check your credit report.

Who's liable?

Federal law limits your liability to \$50 if someone steals and uses your credit card. Some banks don't ever hold you accountable for any fraudulent purchases on your card, so be sure to learn your bank's policy. The rules are a little different if a thief uses your debit or ATM card. You can limit your loss to \$50, but you must report any unauthorized transactions to your bank within two business days of discovering them. If you take longer than two days, you may lose up to \$500, and possibly the entire amount that was debited from your account.

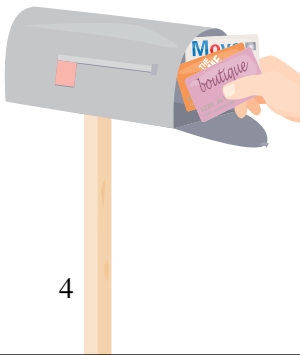
How to protect yourself

One way to reduce your risk of identity theft is learning some of the methods thieves use to steal personal information.

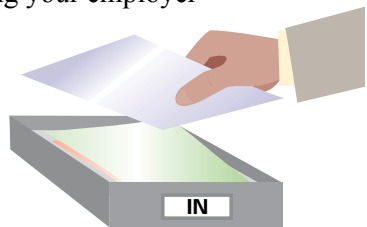


Getting your information without your knowledge

- Stealing bills, bank statements or brokerage summaries, new checks or pre-approved credit card offers from your mail or trash, sometimes called dumpster diving
- Stealing personnel and customer files at business offices, including your employer



card offers from your mail or trash, sometimes called dumpster diving



- Stealing your wallet or purse, or personal documents from your home



- Stealing credit and debit card numbers when your card is swiped through a processing machine, a technique called skimming



- Peering over your shoulder at ATMs to get your PIN number

For these reasons and others, it's a good idea to store your financial paperwork in a safe place at home, and to protect your receipts and bills. You may also want to buy a shredder to destroy sensitive documents when you no longer need them.

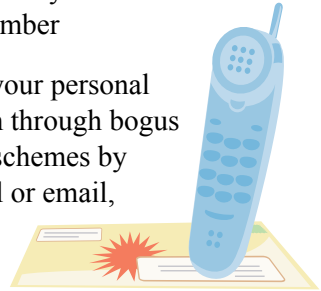
Obtaining your information from other sources

- Filling out a change-of-address form so that they receive mail

addressed to you, including credit card bills for accounts they open but have no intention of paying

- Impersonating your creditors, employers or landlord to obtain a copy of your credit report, which includes your Social Security number

- Obtaining your personal information through bogus marketing schemes by phone, mail or email, sometimes called phishing



- Using advanced technology to breach online security and steal account information

You should be very cautious about giving out your personal information unless you're certain the situation is legitimate. No legitimate financial institution will ask you to confirm your account number or give your Social Security number over the phone or online during a call or communication that you did not initiate.



Preventive measures

You might be surprised by how many ways people might try to steal your personal information. The good news is that there are just as many ways to protect yourself. While following these suggestions will not guarantee you'll be able to prevent identity theft, they'll help minimize your chances of becoming a victim or the damage caused should it occur.

Credit cards and credit accounts

1. Never attach your PIN number to any of your credit or debit cards.
2. Only carry with you the cards,



checks and forms of ID that are absolutely necessary. Keep the others, like your Social Security card and infrequently used credit cards, in a safe place at home.

Paper trail

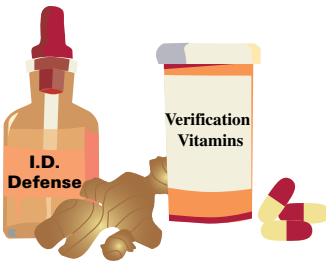
You might think that most identity crimes are committed online. But the FTC reports that only about 20% of all cases involve telecommunications and the Internet. According to the Better Business Bureau's 2005 Identity Fraud Survey Report, 68% of all identity theft cases were committed with information obtained offline. Even more surprising is that in half of the cases in which the identity thief is caught, the crime was committed against someone they know or are related to.

3. Keep a list of all of your credit cards and their customer service telephone numbers in a safe place at home. That way, you can contact the card companies or other lenders immediately with the necessary information if a card is stolen or lost.

4. Monitor your bank accounts and credit card bills closely and regularly for signs of transactions you didn't make. It's a good idea to keep all of your receipts and check them against your printed or online monthly statement.

IDs, bills and credit reports

1. Store your personal identification—your birth certificate, Social Security card and passport—in a safe place at home, especially if you are having service work done to your house. You may wish to consider keeping these under lock and key.
2. Check your credit report at least twice a year, if not more frequently.



3. Shred your receipts and any financial paperwork before you throw them out. The FACT Act requires that by 2007, merchant receipts print no more than the last five digits of a customer's account number.

4. Request that your Social Security number not be used as an account number or for customer, employee or college IDs.
5. Don't leave your outgoing mail in your mailbox to be picked up by your mailperson, as this mail could be stolen. Instead, drop off letters at the post office or in one of their official mailboxes. For the same reason, also be sure to pick up your incoming mail from your mailbox in a timely manner.
6. Do not discuss private, financial matters requiring you to divulge your Social Security number, account numbers or passwords while talking on a cell or cordless phone, as such calls may be intercepted or listened to by potential thieves. Use a landline instead.
7. If you're considering making a donation to a charity, ask for written documentation first and verify the organization's credentials.

Protecting yourself online

You might not realize it, but your personal information is probably stored on your computer at home and work. And if you pay your bills or do any shopping online, you sometimes need to give out your credit information. Although some experts believe your information is safer online than anywhere else, it's still a good idea to take some precautions.

1. Never provide your contact information, login, password or other sensitive information through email. You might receive a phony email that claims to be from a legitimate business, maybe even your bank, and asks for such information. This scam is known as phishing.
2. Consider using a credit card with a Virtual Account Number security feature that generates a different account number every time you make a purchase online.
3. Look for a padlock or key icon at the bottom right of your browser window to ensure you are on a secure page, which means that any personal or credit informa-



tion you provide will be encrypted during the transaction. Some sophisticated thieves have been able to replicate the images, but by double clicking the padlock icon, you can be sure that the URL on the certificate matches the URL of the page you are viewing. If the URLs don't match, it's likely a scam.

FACT Act

The Fair and Accurate Credit Transactions Act (FACT Act) gives you the right to request a free credit report from each of the three major credit bureaus—Equifax, Experian and TransUnion—once a year. To request your report online, visit: www.annualcreditreport.com, or call 1-877-322-8228.

4. Make sure you have up-to-date antivirus software installed on your computer as well as a firewall, especially if you have a high-speed Internet connection that remains connected to the Internet 24 hours a day. Most programs will notify you if there is an update available, but you



What the FTC Says

To learn more about phishing, check out this article from the Federal Trade Commission.

www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.pdf

can also check on your own by visiting the company's website.

What to do if you're a victim

Even if you've taken extra care to guard your personal information, you still might fall victim to identity theft. If so, there are four steps you should follow right away to repair your name and credit. Remember, the faster you respond, the better your chances are of minimizing the damage.

Step 1: Contact one of the three major credit bureaus and place a **fraud alert** on your report. This bureau is then required to notify the other two bureaus to also flag your report. This fraud alert is good for 90 days. It can be extended to 7 years if you provide an identity theft report, as long as

it's filed with a local police agency. Potential creditors will then know to verify any credit requests with you before granting them. If you think your mail has been tampered with, give them your phone number. Once the credit bureau confirms your fraud alert, the two other bureaus will automatically be notified and will place alerts on your report as well. You can request a free copy of your current report from each bureau. Review the reports closely to see what unauthorized accounts were opened and what charges were not paid.

Step 2: File a police report. Most creditors require one when you contact them to clear your credit. If you can't get a copy of the report, get the report number.



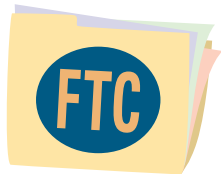
Step 3:

Contact all of the companies you have credit accounts with and close any accounts that have been misused or opened without your authorization. Credit accounts include those with credit card companies, banks, phone companies, wireless companies, Internet service providers (ISPs) and utilities, as well as other service providers.



Step 4: File a complaint with the FTC. Once you do, your information will

be entered into the FTC's secure database and help officials track down thieves. Also, if you were unable to get a copy of the police report, the FTC's ID Theft Affidavit is a standardized five-page form that is accepted by most companies to describe incidents of identity theft.



Where to report fraud

Since it's important to act quickly, it's a good idea to have all the necessary contact information before you need it.

The three major credit bureaus

Equifax

To report fraud, call 1-800-525-6285, and write: P.O. Box 740241 Atlanta, GA 30374-0241 www.equifax.com

Experian

To report fraud, call 1-800-EXPERIAN (397-3742), and write: P.O. Box 9532 Allen, TX 75013 www.experian.com

TransUnion

To report fraud, call 1-800-680-7289, and write: Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92834-6790 www.transunion.com

Federal Trade Commission

To call the FTC's ID Theft Hotline, call 1-877-IDTHEFT (438-4338), and write:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

To file a report with the FTC online, visit: www.consumer.gov/idtheft/

To obtain a copy of the FTC's ID Theft Affidavit online, visit: www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf

Social Security Administration

To report a stolen or misused Social Security number, call 1-800-269-0271 www.ssa.gov

Check Verification Companies

If your checks have been stolen, it's a good idea to notify the following major check verification companies.
TeleCheck
1-800-710-9898

Certegy, Inc.
1-800-437-5120

International Check Services
1-800-366-5010

ChexSystems
1-800-428-9623

Scams and alerts

For updates on current scams and consumer alerts, visit the following websites:

The FTC's ID Theft Home: www.consumer.gov/idtheft/index.html

The Identity Theft Resource Center: www.idtheftcenter.org/index.shtml

Tips to help organize your identity theft case

- Follow up all phone calls you make in writing. Use certified mail, return receipt requested, when you mail the letters. Also keep detailed notes of all conversations you have, including dates, times, name of person you spoke with, etc.
- Keep copies of all letters or forms you mail. If possible, hold on to the originals of supporting documentation, like a police report and letters to and from creditors. Send out copies only.
- Create a filing system for all of your paperwork.
- Store all of your files even after your case is resolved. Problems can arise again, and if they do, you'll be prepared.

As one of the world's leading financial services companies, HSBC is a committed advocate of financial education. Our goal is to help consumers acquire an understanding of financial concepts, as well as the tools necessary to make sound financial decisions. The **YourMoneyCounts**® program, managed by HSBC's Center for Consumer Advocacy, furthers our longstanding commitment to financial education, which dates back to 1929 with the establishment of the Money Management Institute. Recognizing that people choose to learn in different ways, we offer the **YourMoneyCounts** program through multiple channels—online, in print and through financial education workshops.

Visit us at YourMoneyCounts.com

Your**MoneyCounts** is sponsored and managed by HSBC - North America
Your**MoneyCounts** is developed in conjunction with Lightbulb Press®

