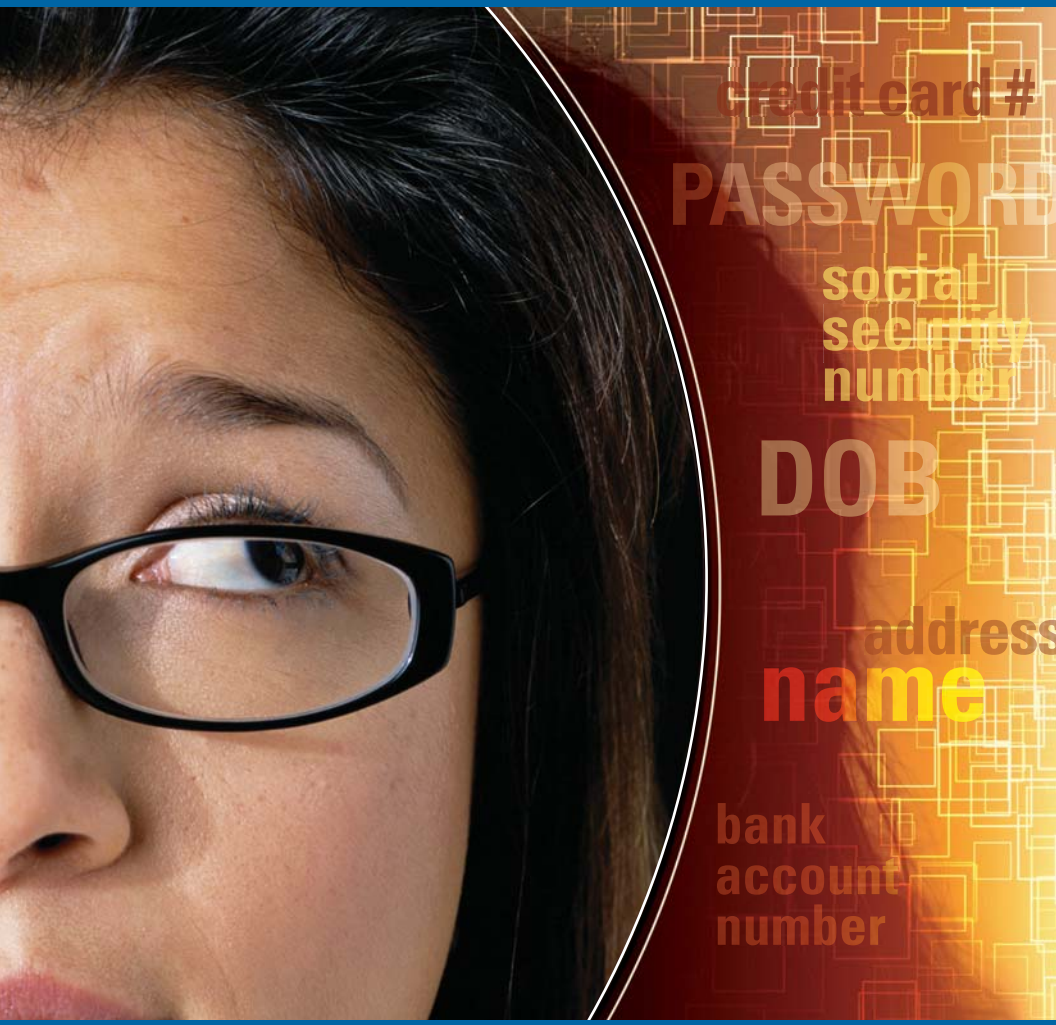
Identity Theft and You



How to prevent and fight identity theft

myFICO®

Identity Theft and You

How to prevent and fight identity theft

The term "identity theft" has been used widely with different meanings. In this booklet, we will define identity theft (also referred to as ID theft) as misuse of another individual's personal information for illicit financial or other gain. This definition is consistent with the approach used by the Federal Trade Commission's Identity Theft Survey Report.[2]

This booklet will give you an easy-to-understand overview of identity theft, as well as ways to prevent, detect and resolve it.

2151EB 04/06 PDF

Why should identity theft concern me?

Identity theft can have a devastating impact on your life, affecting far more than just your pocketbook. If you become a victim of identity theft, you may face problems like these:

- **Money is fraudulently withdrawn from your bank accounts**
- **Your credit score is ruined,** at least for a while, which can increase the interest rate you are charged on loans or credit cards
- **You have difficulty opening bank accounts**
- **You receive annoying calls from collections agencies** for expenses you didn't incur
- **You could end up with a fraudulent criminal record**

How prevalent is ID theft? It has been called the fastest growing white collar crime in America.

Statistics vary widely on the impact of identity theft on American consumers:

- In 2005 alone, it is estimated that nearly 9 million American adults became victims of identity theft, with a total cost of approximately $56 billion to industry and consumers combined[1].
- The Federal Trade Commission estimates that by 2003, 27 million Americans had already been victimized by identity theft[2].

In addition to this direct impact, there are the second-hand effects of identity theft that hurt all of us. For example, we all pay a little more for goods and services because of the cost of fraud to merchants and banks.

Who is most likely to become a victim of identity theft?

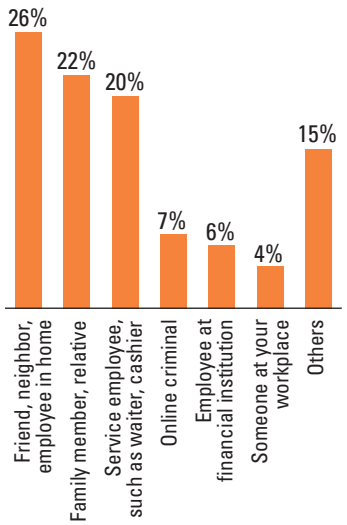
- Statistically, Hispanics and African Americans are more likely than Asian Americans or Caucasians to be victims of fraud. They also experience higher fraud losses.
- Generation X (age 25–34) has a fraud rate of 5.38%, which is higher than other age groups.
- Households that make $150,000 or more per year have higher rates of fraud, but lower average fraud amounts than households with income of under $15,000.[1]

How can I prevent identity theft?

The person stealing your personal information is often someone you know.[1]

Be careful about leaving your information out for all to see.

Criminal's Identity[1]



The best way to keep criminals from misusing your identity is to prevent them from stealing it in the first place. By following a few simple steps, consumers can dramatically reduce the chances of falling victim to identity theft.

Here is an easy way to remember what you need to do to help prevent identity theft: **Secure your Mail, Identifying information, Payment tools, and your Computer.**

To summarize: **Secure MIPC.**

1. Secure your mail.

Both incoming and outgoing mail can be an avenue for identity theft.

- Use a locking mailbox and remove incoming mail promptly.
- Put outgoing mail in an actual postal mailbox rather than simply leaving it in your mailbox at home.
- If you do leave outgoing mail in your mailbox, never put the flag up.
- Shred any mail that has account numbers or "preapproved" credit offers.
- Make sure your trash is in an area that is not easy to access.

2. Secure your personal identifying information.

Remember, the more people who have access to your sensitive personal information, the higher the likelihood of identity theft.

- Be particularly careful with your Social Security number. Don't provide it unless absolutely necessary.
- Don't carry your Social Security card or number in your purse or wallet.
- Shred any documents that contain your Social Security number and other personal information if you no longer need them. Don't just toss them in the trash.
- Write down all your account numbers and keep the list in a safe place so you can easily access the information when you need it.

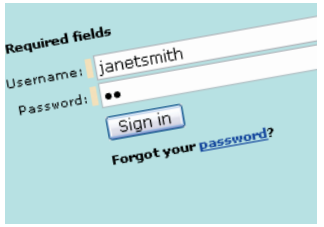
3. Secure the tools you use for making payments.

- Always make sure that all your payment tools such as credit cards, debit cards, checks and account information are secure and not easily accessible, even by friends, relatives and neighbors. Credit card numbers, checking and savings account numbers and personal identification numbers (PINs) can also be misused and should be kept in a similarly safe location.
- Shred documents with financial information such as account numbers rather than just throwing them into the trash.

4. Secure your computer.

Only a relatively small percentage of identity theft occurs online, but you should take reasonable measures to protect yourself.

- Use an anti-virus program and keep it updated.
- Use an anti-spyware software program (many are free).
- Never respond to emails asking for sensitive information or click on links in these emails. If you can, forward the email to the organization that the email claims to be from and have them verify authenticity.
- Don't click on links in emails claiming to have pictures, or the "latest twist" about one of the major stories of the day. Doing so may result in viruses or spyware infecting your computer and possibly tracking and logging your keyboard strokes.
- Don't save your passwords on your computer.



Here's an easy way to remember how to prevent identity theft:

Secure MIPC
(remember it as "secure my PC")

Secure your **M**ail, your **I**dentifying information, your **P**ayment tools, and your **C**omputer.

What's the best way to detect identity theft?

The slowest way to discover fraud is to wait until you're turned down when applying for credit. In these cases, the average loss is $19,735. The average loss when you discover the fraud by reviewing your paper statements is $5,419. And the average loss when you discover fraud by reviewing your statements electronically is $3,806.[1]

When it comes to detecting identity theft, time equals money. If you discover the fraud early, you'll wind up paying less and spending less time cleaning your records and fixing the damage.

Here are some easy steps to help you detect identity theft early and minimize the damage:

1. Check your credit card and bank account balances electronically and often.
You should check them at least once a week. Make sure there are no transactions that are suspicious. You may even want to cancel your paper statements altogether and switch to online statements.

2. Subscribe to an online monitoring service.
These services alert you when there are changes in your credit scores and credit reports or new addresses and phone numbers are reported with your name. Visit *www.myFICO.com* for more information about such services.

3. Check your FICO® scores and credit reports from all three credit reporting agencies.
A FICO® score is a number used by lenders when you apply for credit. It is an estimate of your credit risk based on a snapshot of your credit report at a particular point in time. Your FICO® scores and your credit reports should be checked at least once every year. Checking them every three to six months would be even better. Unexpected drops in your FICO® scores could be caused by the actions of identity thieves. Visit *www.myFICO.com* for comprehensive information about your FICO® scores. You can also visit *www.annualcreditreport.com* to obtain a free credit report from each credit reporting agency.

4. Review your paper statements.
If you do not have access to the internet, carefully review your paper statements for bank accounts and credit cards as soon as you get them. Look for unusual or unfamiliar transactions.

5. Monitor your billing and statement cycles.
Make sure that paper statements are arriving on time and are not missing. If you order new credit or debit cards, keep an eye out for their timely arrival in the mail.

6. Watch out for unexpected phone calls.
If you receive a call from a collection agency for an overdue bill you know nothing about, don't assume it is just a mistake. It may be a sign that your identity has been stolen.

7. Get your FICO® scores and credit reports if turned down unexpectedly for credit.
See whether your FICO® scores have dropped, and examine your credit reports for unusual items that are not a result of actions you have taken. These include new accounts that you didn't open, large balances or delinquencies on existing accounts that you weren't aware of.

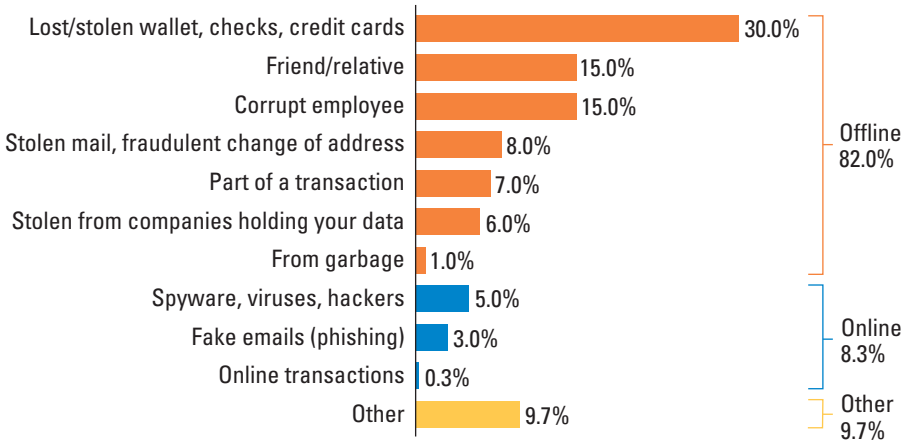
Reviewing statements online helps you detect fraud earlier.

How do identity thieves get my information?

Identity thieves access information through two channels: offline/traditional methods and online/computer.

The offline/traditional methods are those that are carried out without the need for a computer. These may include situations where the criminals steal someone's checks, wallet or purse, or a waiter at a restaurant may use a special device to copy the credit card information for later fraudulent use (skimming).

Methods of Access to Fraud Victims' Information[1]



As its name implies, the online/computer channel involves unauthorized access to sensitive identification and financial information through the computer. This can take different forms, such as sending a spoof email that appears to be from a legitimate financial institution to con you into providing sensitive information (phishing), or sending you to a website other than the one you thought you were going to (pharming).

Once the fraudsters obtain your sensitive identity or financial information through these channels, they can start various fraudulent activities that may include creation of new credit accounts, carrying out fraudulent transactions with existing credit or bank accounts, committing crimes in your name, and more.

Knowing how to spot likely fraudsters and how they get your information, will help you protect yourself against identity theft.

What the financial services industry is doing to protect your credit cards

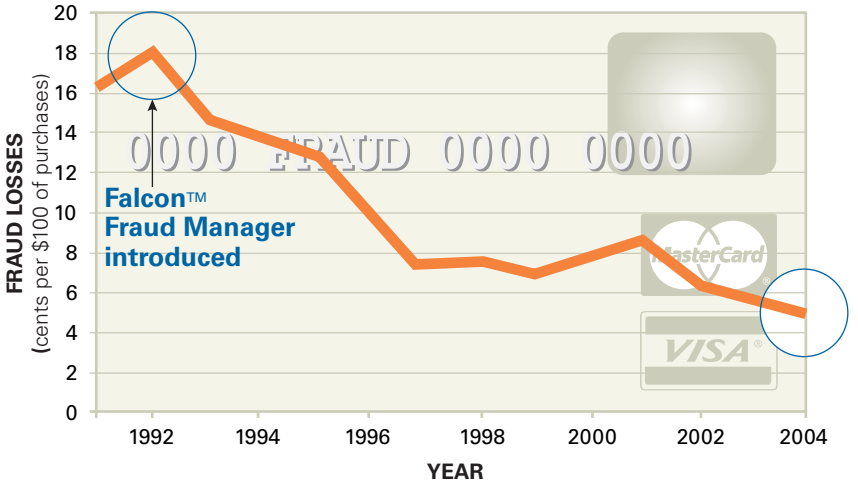
Many of us have received phone calls from our credit card company asking to validate a recent transaction to ensure that we are still in possession of our card and in fact made that particular purchase. This is the result of the bank's fraud detection system identifying a suspicious purchase.

Since the early 1990s banks and credit card issuers have been taking advantage of technology to protect your accounts and reduce fraud. This process has been a major success and has dramatically reduced credit card fraud. In 1992, US credit card issuers were losing $0.18 of every $100 in purchases to credit card fraud. This may seem like a small number, but it adds up to millions of dollars in losses each year. Credit card fraud losses have been reduced over 70% in the past 13 years, and today credit card issuers lose only $0.05 for every $100 in purchases.

The fraud detection system most credit card issuers rely on to protect their customers is **Falcon™ Fraud Manager,** developed by Fair Isaac Corporation. Falcon Fraud Manager protects 85% of credit cards used in the US and 65% of credit cards worldwide.

Falcon Fraud Manager assigns a "fraud score" to credit card and debit card transactions. This score tells the credit card issuers how likely a particular transaction is to be fraudulent. When a transaction is tagged as potentially fraudulent, the bank will often immediately contact you to verify the validity of the transaction.

US Credit Card Fraud Losses (US Visa and MasterCard Accounts)



Case Study: Janice—a young, single professional

Situation	Timeline	Time spent, out-of-pocket expense
Janice is a 34-year-old graphic designer living in California. She is computer-savvy and tends to conduct many of her financial transactions electronically. She worries about identity theft and decides to sign up for a service that alerts her when there are changes in her FICO® score.	February	Less than $10 per month
During a business trip, Janice accidentally loses her purse which contains two credit cards, her driver's license and her medical insurance card which has her Social Security number on it. She discovers the loss the next day when her credit card issuers contact her on her cell phone. They inquire about some unusual transactions and ask whether she has her cards in her possession. She cancels both accounts and is issued new cards. Janice assumes the worst is over.	March 3	30 minutes
A few days later, she receives an email alert from her score monitoring service, notifying her that several credit inquiries have been made in her name, which has caused her FICO® score to drop.	March 10	
Janice uses her monitoring service to obtain all the necessary forms and guidance on what she should do. She obtains copies of all three of her credit reports, and contacts the creditors to whom the identity thief had applied for credit to notify them of the fraud. Because she lives in California, Janice can also place a "freeze" on her credit information, and does so. This prevents the release of this information to almost anyone without her permission. She also reports the fraud to the police and completes an identity theft affidavit with the Federal Trade Commission. Because she acted quickly, Janice is able to limit the amount of the fraud.	March 11–19	6 hours
Janice continues to monitor all her financial accounts electronically at least once every week, and checks her FICO® score and credit report once every month for several months to make sure no more fraudulent actions take place.	May	
Janice's vigilance pays off and no more foul play occurs on her record. But she will continue to monitor her financial records as well as her FICO® score and credit reports on a regular basis.	July	
Total time, out-of-pocket expense		**6.5 hours; Less than $60**

Case Study: Steve and Linda, a married couple

Situation	Timeline	Time spent, out-of-pocket expense
Steve and Linda are married and in their 60s. They have heard about identity theft, but believe it mostly happens to those who make purchases or view their sensitive financial information online. For several years, Steve and Linda have been hiring Dave, the college-age son of one of their long-time neighbors, to help with yard and other handy work around the house. They have known Dave since he was a boy and think nothing of leaving their sensitive information out when he is around. In July, Dave moves out of state to look for a job.	July	
When one of their checks bounces, Steve and Linda review their paper bank statements from the last few months and notice several debit card charges that are unfamiliar to them. The purchases total over $4,000. The bank agrees to refund the majority of the fraudulent transactions, but charges the couple $250 of the costs because they waited well over two months to report the abuse. They are also charged a $25 fee for writing a check with insufficient funds.	October	2 hours; $275
The couple had been planning to apply for an equity line of credit to put in a new deck. They are surprised when they are turned down due to a low FICO® score and bad credit. At about the same time, they start receiving calls from a collection agency inquiring about an overdue credit card bill. They are concerned because they have not used a credit card in many years.	November	
They learn through several interactions with the loan officer and the collection agency and review of their credit reports that someone opened two new credit card accounts in Steve's name several months back, quickly charged over $18,000, and never paid the bills.	December	8 hours
After consulting with friends and asking around, the couple begins to take necessary steps such as filing a police report, completing an affidavit with the Federal Trade Commission, writing letters to the collection agency to dispute the charges on the fraudulent cards, and placing fraud alerts on their credit files.	January (the following year)	40 hours
Meanwhile, the couple discovers that yet a *third* credit card and cellular phone service were obtained in Linda's name in September. They continue writing letters and calling to close these as well.	February	15 hours
In frustration, the couple decides to consult an attorney to help resolve the mess.	February	8 hours; $500
While the worst is over for Steve and Linda, they are still dealing with the aftermath of their ordeal. They will need to gradually rebuild their ruined credit rating before applying for loans. They also have to stay vigilant to prevent further abuse of their good name. They have realized the value of early detection, so they are now checking their account balances electronically once a week.	March	
Total time, out-of-pocket expense		**73 hours; $775**

What should I do if I become a victim of identity theft?

Additional identity theft resources

There are a number of governmental, non-profit, and business organizations that provide identity theft guidance. Contact or website information for some of these resources has been provided.

Fair Isaac's consumer website:
www.myFICO.com

Federal Trade Commission
Phone 877-438-4338
www.consumer.gov/idtheft

US Department of Justice
www.usdoj.gov/criminal/fraud/idtheft.html

Social Security Administration
Phone 800-269-0271
www.ssa.gov

Privacy Rights Clearinghouse
www.privacyrights.org

1. Contact at least one of the credit reporting agencies and request that a fraud alert be placed on your credit reports.
The three major US credit reporting agencies (also known as credit bureaus) are Equifax, Experian and TransUnion. Having a fraud alert on your credit report notifies potential credit grantors to verify your identification before extending credit in your name. (Note that a fraud alert is only a "request." The credit grantors are not legally required to verify your identity). The bureau you contact will pass your request on to the other two major credit bureaus so that the fraud alert appears on your file at all three credit bureaus.

2. If you live in a state that allows you to place a "security freeze" on your credit report, you may want to do so.
The security freeze will prevent the credit bureaus from providing your credit report to *anyone* without your approval (with a few exceptions). Contact the credit bureaus to find out whether your state allows you to use the credit freeze option. There may be a fee for this service.

3. Get copies of all three of your credit reports and examine them carefully.
Look for new accounts the identity thief may have opened, new credit inquiries that represent applications for credit, and misuse of existing accounts such as large unpaid balances on your credit cards. You are entitled to free copies of your credit reports when you become a victim of identity theft. Some states, such as California, enable you to receive one free copy of your credit report per month. Continue to monitor your credit reports for new activities by the identity thieves for several months.

4. Report identity theft to your local police or sheriff's department and get a copy of the police report.
You will likely need to provide a copy of this report to your creditors and the credit bureaus. Make sure you provide comprehensive information to the police, including the account numbers that have been compromised. It would be wise to write down all your account numbers and keep the list in a safe place.

5. Report identity theft to the Federal Trade Commission.
Fill out the Identity Theft Affidavit form. You are likely to need this form in dealing with your creditors.

6. Notify all your credit card issuers as well as your banks and utility providers and let them know you have become a victim of identity theft.
Request that they close any accounts that have been tampered with or you feel may be at risk. Ask for new accounts to be opened in their place.

7. Close any unfamiliar new accounts.
If you identify any new credit or utility accounts the fraudsters have opened in your name, call the issuer or provider and ask that they immediately close them.

8. Call the Social Security Administration.
Contact the Social Security Administration if you suspect that your Social Security number is being used fraudulently.

9. Keep detailed records.
Keep a record of all your correspondences and communications with creditors, credit bureaus, etc., including dates, who you spoke with and what you were told.

Sources
1. Javelin Strategy & Research, Inc., 2006 Identity Fraud Survey Report
2. Federal Trade Commission—Identity Theft Survey Report, September 2003

Additional identity theft resources

Credit reporting agencies

TransUnion
Fraud Victim Assistance Department
Phone: 800-680-7289
Fax: 714-447-6034
P.O. Box 6790
Fullerton, CA 92634-6790

Equifax
Consumer Fraud Division
Phone: 800-525-6285
or 404-885-8000
Fax: 770-375-2821
P.O. Box 740241
Atlanta, GA 30374-0241

Experian
Experian's National
Consumer Assistance
Phone: 888-397-3742
P.O. Box 2104,
Allen, TX 75013

Get the facts about identity theft

Brought to you by

myFICO®

A division of Fair Isaac Corporation

FairIsaac®

Corporate Headquarters:
901 Marquette Avenue, Suite 3200
Minneapolis, MN 55402

www.fairisaac.com
www.myFICO.com