

Fundamentals of PERSONAL FINANCE



Making
informed
financial
choices

Your Guide to Financial Fraud Prevention

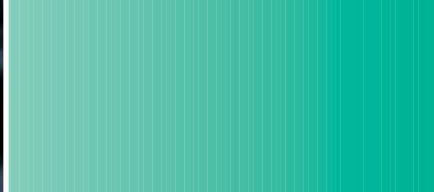
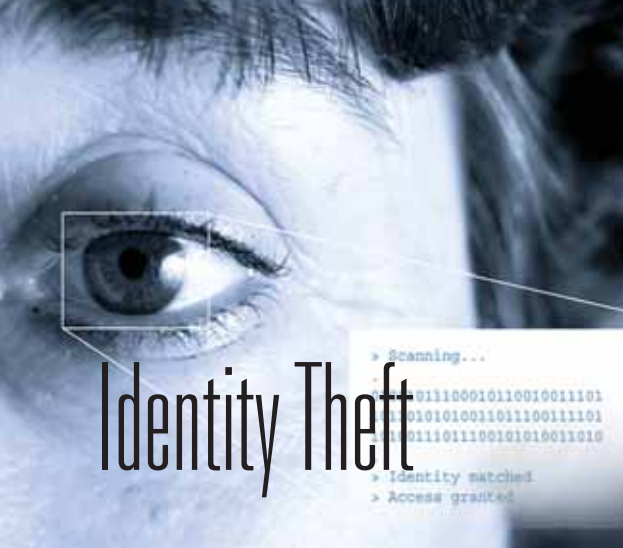


Contents



Your Guide to Financial Fraud Prevention

- Identity Theft 2
- High-Tech Scams 11
- Plastic Card Fraud 15
- Check Fraud 18
- Mail Fraud 21
- Vulnerable Populations 23
- Computer Security 27
- Safe Online Transactions 29
- When You Need Help 31
- Useful Resources 32



Identity Theft

Fraud is everywhere, but you can protect yourself. Financial fraud isn't new. Tricksters always have used ingenious schemes to cheat others out of their hard-earned money.

What's new is that today's technology—which makes it so easy for us to manage and access our money—lets criminals reach into our wallets more easily as well. They can reach us online from around the globe. They can create realistic Web sites or counterfeit credit cards to fool us.

Fortunately, as fast as fraudsters dream up scams to take our money, or even our identities, the good guys—including the folks at your credit union—come up with tools and tips to help you protect yourself. This booklet covers various types of financial fraud and how to guard against them, along with what to do if you are affected.

One of the most prevalent and scary scams is identity theft (ID theft), in

which someone uses another person's name and personal information to commit fraud. Crooks often use stolen information to apply for credit cards and make big purchases.

Some thieves also use a stolen identity (your name, Social Security number [SSN], and possibly other identifying

Crooks use a variety of methods to get the information they need.

information) to get a driver's license, write bad checks, buy a cell phone, rent an apartment, apply for a job, and even drain the victim's credit union/bank account.

The repercussions of ID theft can be very serious, including your being denied credit—such as a home loan, cell phone account, or auto financing—refused a job, or even arrested for a crime someone else committed. Clearing your name is time-consuming, stressful, sometimes costly, and may take months or even years.

Perhaps the most unsettling revelation about identity theft is that, in a large percentage of cases, the thief is someone closely connected to the victim—a co-worker, neighbor, roommate, or even a family member.

Avoid Becoming a Victim

Keeping your SSN out of the wrong hands is a key measure in protecting yourself. “Don't give out your Social Security number unnecessarily,” advises Linda Foley, founder of the Identity Theft

Fraud Warning Signs

Watch for these common warning signs of fraud:

- Letters rejecting you for credit you never applied for
- Missing account statements or charges you don't recognize
- Collection calls for accounts you don't have
- Being denied a job, a rental agreement, loans, or other credit for no clear reason

Resource Center (idtheftcenter.org) in San Diego.

She explains that a SSN is really needed only for tax purposes and to obtain credit. “In every other situation, ask ‘Why do you need it, and what will happen if I don't give it to you?’ If you don't like the answer, take your business elsewhere.”

Other prevention tips include: ►

Crooks, Methods Are Diverse

Crooks use a variety of methods to get the information they need. Some are elaborate ruses to get you to share confidential information, while others are crimes of opportunity.

Some of the low-tech ways thieves get hold of your confidential data include:

- Finding or stealing credit cards, checkbooks, and wallets
- Stealing your mail
- “Dumpster diving” in trash bins for unshredded documents
- “Shoulder surfing” as you punch in your PIN (personal identification number) while using an ATM.

Fraudsters also use high-tech methods such as spoofing, phishing, and vishing to steal your information (see p. 11 for details). In some cases, the theft of your information is completely out of your hands. Security breaches, where thieves steal your information from a company or organization that has your data in its system, happen with alarming frequency.

- Review your credit card and checking account statements each month for unauthorized activities.
- When possible, sign up for e-statements rather than receiving paper ones. (You'll help save a few trees by doing this, too.)
- Make photocopies of financial cards

Keeping your Social Security number out of the wrong hands is a key measure in protecting yourself.

and insurance cards (front and back) that you carry, and keep them in a safe place. Then if your wallet is stolen, you can promptly and accurately report the loss.

- Don't write passwords or PINs on the back of credit or debit cards.
- Limit the information you supply on

entries to win a car or shopping spree. To be eligible to win, information such as your age or income range usually isn't necessary.

- Contact the U.S. Postal Service if you don't receive mail for a few days. You want to confirm that your mail—with, say, preauthorized credit card offers—hasn't been diverted by a thief filling out a change of address form in your name.

- Mail bills from a locked mailbox or at the post office.
- Get off prescreened credit card lists at optoutprescreen.com or dmacconsumers.org.

- Beware of fraudulent e-mails with authentic-looking logos and familiar graphics.

- Never provide your personal information in response to e-mails or phone calls you didn't initiate.

- Make sure shopping Web sites show a closed padlock in the frame of your browser window—separate from the vendor Web site window. URLs (uniform resource locator, or online address) that require a safe connection at checkout start with *https:* or *s-http:*.

Also see the section about young people as targets (p. 6). The tips listed there apply at any age.

Know When You Have to Give a Social Security Number, and When You Don't

Must give SSN

- Credit unions/banks
- Employers
- Income tax records
- Credit bureau reports
- College records
- Loan applications

May want to refuse

- Over the phone
- On personal checks
- On driver's license
- On club membership
- As ID for store purchases
- As general identification

What to Keep and What to Throw Away



ere's a guide to what you should keep, and for how long. When you no longer need these items, crosscut-shred or burn them—remember to shred expired credit cards too.

What to Keep and for How Long

	45 Days	One Year	Six Years	Seven Years	Permanently
Credit card receipts and statements	Keep receipts until your monthly statement arrives; if that's correct, shred the receipts. Exceptions: Keep a receipt if you're disputing a bill or to cover a warranty or return period. Keep the statements for seven years if they contain tax-related expenses.				
Pay check stubs	Make sure the information on your paycheck stubs matches your annual W-2 when you receive it, then shred the stubs. If your employer lists vacation/sick leave carryover on your paycheck stub, keep the last one of the year. Notify your employer if the information doesn't match.				
Retirement/savings plan statements	Keep quarterly statements until you receive your annual summary; if everything is correct on the annual summary, shred the quarterlies. It's best to hold on to annual statements until you retire or close the account. Keep important notices and contacts for retirement plans and pensions permanently.				
Credit union records	At the end of each year, go through your share draft carbons or statements and only keep those related to taxes, business expenses, and housing or mortgage payments.				
Bills	Keep bills for major purchases—cars, jewelry, furniture, computers, and so on—to show proof of their value in the event of loss or damage. For other bills, once you know payment has cleared your credit union for a particular bill and the return/refund period has expired, shred that bill.				
House records	Keep purchase price information and the cost of permanent improvements to your property, such as remodeling. Also, if you buy or sell property, keep records of legal fees and your real estate agent's commission for six years after you sell your house. Keeping these records, especially home improvement records, is a good idea and could potentially assist you in lower capital gains tax should you decide to sell.				
Tax records	The IRS has three years to audit your return, and you have three years to file an amended return to claim a refund if you made a mistake. If you made the mistake of underreporting your gross income by 25% or more on a return, the IRS has six years to challenge it. If you filed a fraudulent return or didn't file one at all, the IRS can catch you on it at any time. Keep a copy of all 1040 tax forms permanently.				
IRA contributions	Keep nondeductible contribution records permanently in case you need to prove you paid tax on the money when you want to withdraw it.				

Miscellaneous

Also keep these permanently: Updated household inventory, birth and death certificates, marriage license, divorce papers, military records, insurance claims, accident reports and claims, proof of ownership and major debt repayment, and legal correspondence.

 Recommended time to keep documents
  Some cases call for longer retention

Another major piece of the prevention puzzle is checking your credit report every year, free, through *annualcreditreport.com*; 877-322-8228. When you receive your credit report, verify that it's accurate and includes only activities you've authorized.

Also check reports under your child's name to ensure no one is misusing it. Finding out sooner rather than later that someone has hijacked your identity—or your child's—allows you to shift into damage control mode.

Stagger Your Credit Report Requests

You're entitled to a free credit report annually from each of the three national credit bureaus—Equifax, Experian, and

TransUnion (see the box on p. 10 for details). Instead of ordering all three at once, spread the requests out over the year. Order one in January, one in May, and one in September. This will help you monitor for signs of identity theft year round.

Too Young To Be a Target? Think Again

While anyone with a Social Security number is a potential ID victim, teens and young adults may be particularly vulnerable to scammers. Consumers between the ages of 18 and 29 now make up one of the largest target groups for identity thieves, according to the Federal Trade Commission's (FTC) numbers. So if you fall into that age

Medical ID Theft Threatens Your Money and Your Life

It's bad enough to open your credit card bill and find a long list of charges that you didn't make. But what if you get a hospital bill demanding payment for an operation you never had? What if, instead of your credit card number, someone has used your identity to receive costly medical care?

This is medical identity theft. The crime is not yet widespread—the World Privacy Forum, San Diego, estimates that medical ID theft has affected 250,000 Americans in recent years. It is, however, a crime whose victims bear enduring and maybe fatal consequences. It's also one from which we have too little legal protection and against which we have even less legal recourse.



Providers will absorb the loss once they have proof of the fraud. But the law doesn't make it easy for victims to get that proof. Meanwhile, your credit

group, watch your back to avoid becoming another statistic.

“Young people can be more exposed to the potential for identity theft than some other age groups,” says Linda Foley, founder of the Identity Theft Resource Center (*idtheftcenter.org*) in San Diego. “And when you’re young, you have this sense of being immortal ... this couldn’t happen to me.”

Your generation’s close relationship with technology is a factor. Crooks today develop complex schemes that exploit your preference to be plugged in—something your parents never had to contend with.

Experts and advocates acknowledge that you can’t completely prevent identity theft, but they all agree you can significantly reduce your risk by following these tips:

- Ask school administrators to assign you a student ID number other than your SSN.

record may be permanently damaged.

There are dire medical consequences, too. After the ID theft, your medical records no longer are your own. Your name is on the files and the insurance claims, but only some of the information in them is yours. The rest belongs to the criminal who used your name and insurance information. That thief’s information literally could kill you if it results in your getting improper medical treatment. Inaccurate claims and medical information also can cost you a job or make you ineligible for health or disability insurance. And it’s almost impossible for you to remove it from your record.

Where do you go for help? The Fair Credit Reporting Act, which gives you the right to see your credit scores and reports, dispute frauds, correct inaccuracies, and more, can help you deal

Teens and young adults may be particularly vulnerable to scammers.

- Don’t leave your purse, wallet, or backpack unattended.
- Don’t carry your Social Security card or birth certificate with you.
- Send and receive mail in a mailbox that’s inaccessible to crooks.
- Cross-cut shred unwanted credit card offers and any document that reveals information a crook could use.
- At home, keep all confidential information out of sight.
- Don’t submit credit applications at campus kiosks.
- Check your credit report to make

with financial aspects of medical ID theft—once you prove the charges are fraudulent.

Unfortunately, you need to see your medical records to do that. No law will help you do that. Especially not the privacy rule of the Health Insurance Portability and Accountability Act (HIPAA). According to consumer and privacy advocates, HIPAA is little more than a dull double-edged sword when it comes to medical ID theft.

HIPAA was enacted, in part, to make sure that health-care and insurance providers protect your private health information from such abuse. But because of a loophole in the rule, once you prove that your record includes someone *else’s* information, your right to see it and correct it ends. The law that should have protected you turns around and protects the thief.

sure no one is misusing your name (see ID theft prevention tips and resource box, p. 3).

- Create passwords that use a combination of letters (upper and lower case), symbols, and numbers.
- Don't respond to e-mail messages asking for personal information, or click on links within e-mail messages you weren't expecting.
- Never include your SSN in an online résumé or other posting.
- Log out completely whenever you leave a computer.
- Before you get rid of an old computer, delete all your personal information by overwriting the entire hard drive with shredding software.
- Use online account access to check routinely for transactions made by others. Technology can be your primary defense against crooks.

As many twenty-somethings have learned the hard way, you're not too young to attract a thief. Protect your personal information so that ID theft doesn't distract you from what's really important—preparing for a bright future.

If You're a Victim

What if it does happen to you? Say someone stole your name, SSN, and credit card number, bought a townhouse in Monte Carlo, and started commuting to the local jewelry store in a new Ferrari that was, yes, also billed to your account.

What can you do about it? You can notice and report the theft quickly, reject the fraudulent charges, restore your good name, and protect against future fraud.

The identity theft counter-offensive has two goals: To restore your good name and to make sure you don't wind up paying for Ferraris driven by anonymous thieves. Unfortunately, you'll

largely be left to your own devices; while you should contact the FTC, and probably your local police, the government will provide limited help.

But if you know the rules, act fast, and work carefully, your main cost will

Consumers ages 18 to 29
make up one of the largest
target groups for ID thieves.

be time spent. Otherwise, the effort, confusion, frustration, and expense of an identity theft can last for years.

To Catch a Thief

At the first signal that you may be a victim, take action. Alert one of the credit reporting agencies, which is obliged to notify the others, about the suspected identity theft (see p. 10 for details). Direct the agency to place a "90-day fraud alert" on your account. This will require financial firms to get extra identification from applicants before opening an account or establishing credit in your name. You may extend this fraud alert to a seven-year alert by writing to the credit reporting agency. You may issue consecutive 90-day alerts if you don't want to issue a seven-year alert.

If you suspect that someone's been using your SSN, contact the Social Security Administration to verify the accuracy of your reported earnings and your name. Follow each conversation with a certified letter, return receipt requested, and keep copies.

Contact creditors, utilities, and financial institutions about fraudulent accounts. Close affected accounts and open new ones using new passwords and PINs.

After you close compromised credit accounts, confirm the action by mailing the FTC's identity-theft affidavit for each account. On all correspondence, include your name, address, account number, and the amount, date, and explanation for the fraudulent charges. Unless directed otherwise, use the address listed for "billing inquiries," not the payment address.

The Fair Credit Billing Act governs

credit card disputes. In most cases, liability is limited to \$50 for each credit card—if you contact the issuer within 60 days of the bill's arrival (or normal arrival date).

Once you notify the financial institution, the first step in fighting fraudulent credit union and bank transactions (such as unauthorized withdrawals) is to check jurisdiction: Federal law governs electronic transfers, while state law governs "paper" withdrawals.

Try to report lost or stolen ATM and debit cards within two business days. The longer you wait, the larger your financial liability. While state laws vary

Freeze Out Thieves

M

ost lenders review applications for credit by obtaining a credit report from one of the three major credit reporting bureaus: Experian, Equifax, or TransUnion (see p. 6 for details).

You can place a credit freeze, sometimes called a "security freeze," to block the credit bureaus from releasing a credit report, which helps prevent identity thieves from misusing your personal information to gain access to new forms of credit issued in your name. You must block each credit report separately.

If you want to obtain a new credit card or loan, you must temporarily or permanently remove the credit freeze.

Credit freeze legislation is passed on a state-by-state basis, with state fees for placing or lifting a freeze with each credit bureau ranging from free to \$10. Some states lower or waive fees for identity theft victims.

In states that lack credit freeze rules, consumers can use voluntary programs from the three credit bureaus. Each charge \$10 for placing or lifting a freeze.

Check the rules and fees for getting a credit freeze in your state by visiting *consumersunion.org*. Click on the "Money" tab and select "Financial Privacy Now." Look for the "Security Freeze" section and click on "State Security Freeze Laws."

Weigh the costs of getting a credit freeze against the benefits for your situation. You already have other options that can help protect your credit:

- Place a "fraud alert" on your credit report to tell businesses you have concerns about ID theft (see p. 8). Visit the FTC Web site for more information.
- Opt out of "preapproved" offers from credit card and insurance companies to prevent identity thieves from intercepting these mailings. Call 888-567-8688 toll-free.
- Protect personal information. Keep personal records in a secure location, never share sensitive information with callers or via e-mail, and shred discarded documents.
- Monitor your credit report and financial accounts to spot potential fraud.