Broadview
Federal Credit Union

Fraud Prevention

Broadview
Federal Credit Union

The mission of Broadview Financial Well-Being is to guide and encourage individuals to focus on achieving economic stability—using innovative tools, making informed decisions, and encouraging positive habits.

Broadview Financial Well-Being learning content and activities are aligned to the applicable K-12 educational learning standards: The New York State Learning Standards: Career Development and Occupational Studies; The National Standards in K-12 Personal Finance Education; and the NYS Next Generation Learning Standards; or the applicable adult learning standards: Institute for Financial Literacy: National Standards for Adult Financial Literacy Education.

The following resources were used in compiling this publication:

Content courtesy of The Federal Trade Commission, adapted from articles on its "Consumer Alerts" website, https://www.consumer.ftc.gov/consumer-alerts.*
- https://www.consumer.ftc.gov/articles/0090-using-money-transfer-services
- https://www.consumer.ftc.gov/articles/0003-phishing
- https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs
- https://www.consumer.ftc.gov/articles/0171-medical-identity-theft
- https://www.consumer.ftc.gov/articles/0008-tax-related-identity-theft
- https://www.consumer.ftc.gov/articles/0040-child-identity-theft

Content courtesy of AARP, adapted from an article on its website, https://www.aarp.org/health/drugs-supplements/info-2024/fake-medications-from-online-pharmacies.html?msockid=2eec4d10f6806bc3315b5976f7996a45

*Some of these articles also may be available in Spanish: La Comisión Federal de Comercio, https://www.consumidor.ftc.gov/. Información para consumidores

Content courtesy of National Council on Aging, adapted from articles on its website, https://www.ncoa.org/:
- https://www.ncoa.org/economic-security/money-management/scams-security/top-10-scams-targeting-seniors

Today's world is full of technological advances that can add conveniences to our lives and help us do more in less time. Much of that activity involves the use of our personal information such as: name, address, credit card numbers, checking account information, and even Social Security numbers. While reputable sites and companies are diligent about protecting that information, there is a perpetual risk of outsiders with malicious intent, who will try to hack even the best systems and steal your information for their own gain.

It is best to have some basic information so that you can protect yourself and your hard-earned income and assets. Some methods of fraud are high-tech and others may surprise you with their simplicity. We sincerely hope that you never have to deal with scams and identity theft. However, it is important to be prepared and aware so that you can protect the assets you build throughout your life. This booklet provides information about how to avoid identity theft or fraud, and guide you on steps to take if you do become a victim.

Table of Contents

Common Scam Tactics

Phone Calls and Text Messages:

Phone contact can be an effective way to cheat the unsuspecting person out of their personal information or their hard-earned money. These scammers make hundreds of calls each day, ready to strike with the person who doesn't disconnect the call and, instead, "buys" the story.

You're Being Sued By the IRS

You get a call or voicemail from someone claiming to be from the IRS. They say you're being sued and this is your final notice. Don't panic. And don't return the call. It's a scam. If you're not sure whether a call is really from the IRS, you can double-check by calling the IRS directly at 1-800-829-1040 or with the Treasury Inspector General for Tax Administration (TIGTA) at www.tigta.gov.

REMEMBER:

- If the IRS needs to contact you, they'll do it by mail first. The IRS won't demand personal information, like credit card or Social Security numbers, over the phone or by email, text or social media messages.
- The IRS won't threaten to arrest or sue you, or demand that you pay right away.
- The IRS won't tell you to use a specific form of payment like a money transfer from MoneyGram, Western Union, or a gift card. Scammers ask you to use those ways to pay because it is hard to track or cancel these payments.

Unfamiliar Robocalls

If you pick up the phone and hear a recorded sales pitch, hang up and report it to the FTC at www.ftc.gov/complaint. These calls are illegal, yet plentiful. Don't press 1, 2 or any number to get off a list or speak to a person. That just means you'll get even more calls.

Can You Trust Your Caller ID?

Scammers can make caller ID look like anyone is calling: the IRS, a business or government office...even your own phone number. If they tell you to pay money for any reason, or ask for your financial account numbers, hang up. If you think the caller might be legitimate, call back to a number you know is genuine—not the number the caller gave you.

Telemarketing Scams

Scammers use fake telemarketing calls to prey on people who may be persuaded to make a purchase over the phone. With no face-to-face interaction and no paper trail, these scams are incredibly hard to trace. Also, once a successful deal has been made, the buyer's name is shared with similar schemers looking for easy targets, sometimes defrauding the same person repeatedly.

Examples of telemarketing fraud include:

The Pigeon Drop—The con artist tells the individual that he/she has found a large sum of money and is willing to split it if the person will make a "good faith" payment by withdrawing funds from his/her bank account. Often, a second con artist is involved, posing as a lawyer, banker, or some other trustworthy stranger.

The Fake Accident Ploy—The con artist gets the victim to wire or send money on the pretext that the person's child or another relative is in danger and needs the money.

Charity Scams—Money is solicited for fake charities. This often occurs after natural disasters or during other humanitarian relief campaigns.

On the Internet:

Fake Anti-Virus Tools

Pop-up browser windows simulating virus-scanning software can fool victims into either downloading a fake anti-virus program (at a substantial cost) or an actual virus, which will expose information on the user's device to scammers.

Email Scams and Phishing

Email (and text message) scams commonly appear as messages from a seemingly legitimate company, asking you to "update" or "verify" your personal information. These messages may also be sent appearing to be from the IRS about a tax refund. When Internet fraudsters impersonate a business to trick you into giving out your personal information it is called "phishing". Do not reply to any email, text, or pop-up message that asks for your personal or financial information. Do not click on links within them, even if the message seems to be from an organization you trust. It isn't. Legitimate businesses don't ask you to send sensitive information through insecure channels.

Examples of phishing messages might look like this:

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

Money Transfer Scams

Money transfers may be useful when you want to send funds to someone you know and trust, but they're never a good idea when you're dealing with a stranger.

Scam artists use a number of elaborate schemes to get your money, and many involve money transfers through companies like Western Union and MoneyGram.

Scammers pressure people to use money transfers so they can get the money before their victims realize they've been cheated. Money transfers are virtually the same as sending cash — there are no protections for the sender. Typically, there is no way you can reverse the transaction or trace the money.

Fake check scams are another popular way scammers try to engage you in a money transfer. Someone sends you a check with instructions to deposit it and wire some or all the money back. The check is fake, but it may look legitimate and may get past a bank teller. You can usually get cash before the bank discovers the fraud, as it can take several days to uncover a fake check due to standard processing procedures. You are responsible for the checks you deposit, so if a check turns out to be fraudulent you will owe the bank any money you withdrew.

These scams may be presented in one of these ways: Lotteries and Sweepstakes, Overpayment Scams and Mystery Shopper Scams.

Don't do it! The checks, the lottery, the overpayment, and the "mystery shopping" job are all fake, and put you at risk for losing your money.

Financial Scams That Target Seniors

Seniors are thought to have a significant amount of money sitting in their accounts. Financial scams targeting seniors have become so prevalent that they're now considered "the crime of the 21st century".

These scams often go unreported or can be difficult to prosecute, so they're considered a "low-risk" crime to the scammer. However, they're devastating to many older adults and can leave them in a very vulnerable position with little time to recoup their losses.

Medicare/Health Insurance Scams

Every U.S. citizen or permanent resident over age 65 qualifies for Medicare, so there is rarely any need for a scam artist to research health insurance information for older people in order to scam them out of some money.

In these types of scams, perpetrators may pose as a Medicare representative or they will offer bogus services for elderly people at makeshift mobile clinics. In either scenario the senior provides their personal information, which is then used by the scammer to bill Medicare and pocket the money.

Counterfeit Prescription Drugs

Most commonly, counterfeit drug scams operate on the Internet, where people may go to find better prices on medications. The National Association of Boards of Pharmacy warns that 95 percent of websites offering prescription-only drugs are operating illegally. The danger is that, besides paying money for something that will not help a person's medical condition, victims may purchase unsafe substances that can inflict even more harm. A legitimate online pharmacy always requires a doctor's prescription. provides a physical address and telephone number in the U.S., has a licensed pharmacist on staff to answer your questions, is licensed with a state board of pharmacy.

Funeral and Cemetery Scams

The FBI warns about two types of funeral and cemetery fraud perpetrated on seniors. In one approach, scammers read obituaries and call or attend the funeral service of a complete stranger to take advantage of the grieving widow or widower. Claiming the deceased had an outstanding debt with them, scammers will try to extort money from relatives to settle the fake debts. A tactic of disreputable funeral homes is to capitalize on family members' unfamiliarity with the considerable cost of funeral services to add unnecessary charges to the bill.

Investment Schemes

Because many seniors find themselves planning for retirement and managing their savings once they finish working, a number of investment schemes have been targeted at seniors looking to safeguard their cash for their later years. From pyramid schemes to fables of a Nigerian prince looking for a partner to claim inheritance money, to complex financial products that many economists don't even understand - investment schemes have long been a successful way to take advantage of older people.

Homeowner/Reverse Mortgage Scams

Scammers like to take advantage of the fact that many older adults own their homes, a valuable asset that increases the potential dollar value of these crimes. A particularly elaborate property tax scam in San Diego saw fraudsters sending personalized letters to different properties, apparently on behalf of the County Assessor's Office. The letter, made to look official but displaying only public information, would identify the property's assessed value and offer the homeowner a reassessment of the property's value and therefore the tax burden associated with it. The scammer collects a fee for this bogus service, preying on the homeowner's hope of reduced taxes.

Scammers are taking advantage of the gaining popularity of reverse mortgages. Several variations may be disguised as opportunities for investing, house flipping, home improvement, foreclosure avoidance, or special financing for military veterans. As opposed to official refinancing, however, unsecured reverse mortgages can lead property owners to lose their homes when the perpetrators offer money or a free house somewhere else in exchange for the title to the property.

The Grandparent Scam

The grandparent scam is so simple and so devious because it uses one of older adults' most reliable assets, their hearts. Scammers will place a call to an older person and will say something along the lines of: "Hi Grandma, do you know who this is?" When the unsuspecting grandparent guesses the name of the grandchild the scammer most sounds like, the scammer has established a fake identity without having done a lick of background research. Advances in voice spoofing using artificial intelligence further complicate detection of the scammer.

Once "in," the fake grandchild will usually ask for money to solve some unexpected financial problem (overdue rent, payment for car repairs, etc.), to be paid via Western Union or MoneyGram, which don't always require identification to collect. At the same time, the scam artist will beg the grandparent "Please don't tell my parents, or I will be in a lot of trouble." While the sums from such a scam are likely to be in the hundreds, the very fact that no research is needed makes this a scam that can be perpetrated over and over at very little cost to the scammer.

NOTES:

Steps to Take If You or Your Elder is a Victim of a Scam.

If you think you or a loved one has been scammed, don't be afraid or embarrassed to talk about it—waiting could only make it worse. Below are some of your best courses of action:

- Call your financial institution or credit card company if you used one of your accounts.
- Cancel any debit or credit cards linked to the account you may have used.
- Reset your personal identification numbers.
- Contact a consumer protection office in your area. These offices not only contain information about consumer scams, but also provide a variety of services such as investigating and prosecuting scammers according to criminal law.
- Report the scam to the police and/or local prosecutors.
- Contact the National Fraud Information Center: www.fraud.org. The NFIC accepts reports about attempts to defraud consumers on the phone or the Internet.
- Contact the Better Business Bureau: www.bbb.org.
- Consider contacting www.justice.gov/criminal-fraud/report-fraud or the FBI depending on the type of fraud.

Identity Theft

According to the Federal Trade Commission (FTC), identity theft happens when someone steals your personal information and uses it without your permission.

It is a serious crime that can wreak havoc with your finances, credit history and reputation—and it can take time, money and patience to resolve. Thieves are resourceful and use a variety of ways to get your information.

If you suspect that someone has stolen your identity, acting quickly is the best way to limit the damage. Setting things straight involves some work.

What Do Thieves Do With Your Information?

Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.

Other Kinds of Identify Theft

Medical Identity Theft

A thief may use your name or health insurance numbers to: see a doctor; get prescription drugs or file insurance claims. Read your medical and insurance statements regularly and completely, as they can show warning signs of identity theft. Check the name of the provider, the date of service, and the service provided. Do the claims match the care you received? Report any mistakes to your health plan.

Tax-Related Identity Theft

An identity thief may use your Social Security number to get a tax refund or a job. Contact the IRS if they send you a notice saying their records show:

- You were paid by an employer you don't know.
- More than one tax return was filed using your Social Security number.

Child Identity Theft

A child's Social Security number can be used by identity thieves to apply for government benefits, open bank and credit card accounts, apply for a loan or utility service, or rent a place to live. Your child's personal information is protected by law, but it is still vulnerable to scammers.

Clues That Someone Has Stolen Your (or Your Child's) Information

- You see withdrawals from your bank account that you can't explain.
- You don't get your bills or other mail.
- Merchants refuse your checks.
- Debt collectors call you about debts that aren't yours.
- You find unfamiliar accounts or charges on your credit report.
- Medical providers bill you for services you didn't use.
- Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.
- A health plan won't cover you because your medical records show a condition you don't have.
- The IRS notifies you that more than one tax return was filed in your name, that you have income from an employer you don't work for, or your child didn't pay income taxes.
- You (or your child) are denied government benefits because they are being paid to another account using your (or your child's) Social Security number.
- You receive collection calls or bills for products or services you didn't receive.

Tips to Protect Yourself

Protecting your personal information can help reduce your risk of identity theft. There are four main ways to do it: know who you share information with; store and dispose of your personal information securely, especially your Social Security number; ask questions before deciding to share your personal information; and maintain appropriate security on your computers and other electronic devices.

Securing Your Information in General

Limit what you carry. When you go out, take only the identification, credit, and debit cards you need. Leave your Social Security card at home. Make a copy of your Medicare card and black out all but the last four digits on the copy. Carry the copy with you, unless you are going to use your card at the doctor's office.

Secure financial documents. Everyone is at risk of financial abuse, regardless of income or assets. Lock your financial documents and records in a safe place at home, and lock your wallet or purse in a safe place at work. Keep your information secure from anyone who enters your home.

Deter solicitors. Always tell them: "I never buy from (or give to) anyone who calls or visits me unannounced. Send me something in writing." Don't buy from an unfamiliar company and always ask for and wait until you receive written material about any offer or charity. And always take your time in making a decision.

Shred sensitive documents. Destroy all receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, and similar documents when you don't need them any longer. Invest in—and use—a cross-cut paper shredder, and monitor your bank and credit card transactions..

Sign up for the "Do Not Call" list. Visit Do Not Call (www.DoNotCall.gov) to stop telemarketers from contacting you, and be careful with your mail. Also take yourself off unwanted mailing lists.

Reduce the risks related to mail. Promptly remove incoming mail from your mailbox. If you won't be home for several days, request a vacation hold (www.usps.com/holdmail) on your mail.

Use direct deposit whenever possible. This ensures that checks go right into your accounts and are protected. Clever scammers have been known to steal checks right out of mailboxes, and even unscrupulous loved ones or caretakers may steal from an elder's home if checks are laying around.

Protect your health coverage information. In the wrong hands, this is as damaging as a thief with your credit card, banking, and Social Security numbers. Misuse of Medicare dollars is one of the largest scams involving seniors. Common schemes include billing for services never delivered and selling unneeded devices or services to beneficiaries. Review medical statements to be sure you have actually received the services billed.

Watch for phone phishing. Never give your credit card, banking, Social Security, Medicare, or other personal information over the phone unless you initiated the call. Don't share your health plan information with anyone who offers free health services or products. Be wary of salespeople trying to sell you something they claim will be paid for by Medicare or other insurance.

Ask questions before sharing your personal data.

Before you share information at your workplace, a business, your child's school, or a doctor's office, ask why they need it, how they will safeguard it, and the consequences of not sharing.

Tips to Protect Yourself, cont.

Securing Your Information Online

Be alert to impersonators. Know who is getting your personal or financial information. Don't give it out on the phone, through the mail or over the Internet unless you've initiated the contact or know who you're dealing with. If a company that claims to have an account with you sends email asking for personal information, don't click on links in the email. Instead, seek a verified source (like their website or your account statement) for their customer service department contact information. Ask if the company really sent a request.

Safely dispose of personal information. Before you dispose of a computer, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive. Before you dispose of a mobile device, check your owner's manual, the service provider's website, or the device manufacturer's website for information on how to delete information permanently, and how to save or transfer information to a new device. Remove the memory or subscriber identity module (SIM) card from a mobile device. Remove the phone book, lists of calls made and received, voicemails, messages sent and received, organizer folders, web search history, and photos.

Encrypt your data. Keep your browser secure. To guard your online transactions, use encryption software that scrambles information you send over the Internet. A "lock" icon on the status bar of your Internet browser means your information will be safe when it's transmitted. Look for the lock before you send personal or financial information online.

Keep passwords private. Use strong passwords with your laptop, credit, bank, and other accounts. Be creative: think of a special phrase and use the first letter of each word as your password. Substitute numbers for some words or letters. For example, "I want to see the Pacific Ocean" could become "1W2CtPo".

Don't over share on social networking sites. If you post too much information about yourself, an identity thief can find information about your life, use it to answer "challenge" questions on your accounts, and get access to your money and personal information. Consider limiting access to your networking page to a small group of people. Never post your full name, Social Security number, address, phone number, or account numbers in publicly accessible sites.

Securing Your Social Security Number.

Keep a close hold on your Social Security number and ask questions before deciding to share it. Ask if you can use a different kind of identification. If someone asks you to share your SSN or your child's, ask:

- Why they need it.
- How it will be used.
- How they will protect it.
- What happens if you don't share the number.

The decision to share is yours. A business may not provide you with a service or benefit if you don't provide your number. Sometimes you will have to share your number. Your employer and financial institutions need your SSN for wage and tax reporting purposes. A business may ask for your SSN so they can check your credit when you apply for a loan, rent an apartment, or sign up for utility service.

Keeping Your Devices Secure

Use security software. Install anti-virus software, anti-spyware software, and a firewall. Set your preference to update these protections often. Protect against intrusions and infections that can compromise your computer files or passwords by installing security patches for your operating system and other software programs.

Avoid phishing emails. Don't open files, click on links, or download programs sent by strangers. Opening a file from someone you don't know could expose your system to a computer virus or spyware that captures your passwords or other information you type.

Be wise about WiFi. Before you send personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected.

Lock up your laptop. Keep financial information on your laptop only when necessary. Don't use an automatic login feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it will be harder for a thief to get at your personal information.

Protect Your Loved Ones: Signs to Look For

If you know or care for an older adult, here are some additional warning signs that may indicate they are the victim of financial abuse:

- There are unusual recent changes in the person's accounts, including atypical withdrawals, new person(s) added, or sudden use of a senior's ATM or credit card.
- The senior suddenly appears confused, unkempt, and afraid.
- Utility, rent, mortgage, medical, or other essential bills are unpaid despite adequate income.
- A caregiver will not allow others access to the senior.
- There are piled up sweepstakes mailings, magazine subscriptions, or "free gifts," which means they may be on "sucker lists."

Every state operates an Adult Protective Services (APS) program, which is responsible for receiving and investigating reports of elder abuse, neglect, and exploitation, and in most states, the abuse of younger adults with severe disabilities. APS is the "911" for elder abuse. Anyone who suspects elder abuse, neglect, or exploitation should make a report. The reporter's identity is protected. APS services are confidential, so the reporter may not be able to learn the outcome of the case. APS respects the right of older persons to make their own decisions and to live their lives on their own terms. In cases of cognitive impairment, however, APS will take steps to protect the older person to the degree possible.

NOTES:

What to Do
If You Are a Victim of Identity Theft

If you believe you have been a victim of identity theft, take action right away!

- If your wallet, Social Security card or other personal, financial or account information is lost or stolen, contact the credit reporting companies and place a fraud alert on your credit file. Check your bank and other account statements for unusual activity.
- If your information is lost in a data breach, the organization that lost your information will notify you and tell you about your rights. Generally, you may choose to place a fraud alert on your credit file, monitor your accounts for unusual activity and exercise your free right to a copy of your credit report. The alert tells potential creditors and lenders to contact you directly and verify your identity before opening new accounts in your name. You can renew the fraud alert after one year, or remove it at any time.
- Visit **IdentityTheft.gov** if you believe you have been the victim of identity theft, or if your personal information has been lost or exposed. IdentityTheft.gov is the government's free, one-stop resource for reporting and recovering from identity theft. The website, available in Spanish at ***RobodeIdentidad.gov***, will provide you with a personal, interactive recovery plan tailored to your individual identity theft needs. It will:
  - Walk you through each recovery step.
  - Generate pre-filled letters, affidavits, and forms for you to send to credit bureaus, businesses, debt collectors, and the IRS.
  - Adapt to your changing needs, provide you with follow-up reminders, and help you track your progress.
  - Provide advice about what to do if you're affected by specific data breaches.
  - **IdentityTheft.gov** has recovery plans for more than 30 types of identity theft, including tax-related identity theft and identity theft involving a child's information.

If you think someone used your SSN for a tax refund or a job—or the IRS sends you a notice or letter indicating a problem—contact the IRS immediately. Specialists will work with you to get your tax return filed, get you any refund you are due, and protect your IRS account from identity thieves in the future.

1. Contact the IRS Identity Protection Specialized Unit **(www.irs.gov/identitytheft)** or call 800-908-4490 to report the fraud. Send a copy of your police report or an "IRS ID Theft Affidavit Form 14039" (you can find this PDF online by searching the title) and proof of your identity, such as a copy of your Social Security card, driver's license or passport.
2. Update your files. Record the dates you made calls or sent letters. Keep copies of letters in your files.

For information regarding your credit report or questions contact any of the following credit reporting agency (CRA)—(Experian, TransUnion, Equifax). If your credit reports shows information is being misused, call each agency and ask them to remove all accounts, inquiries, and collection notices from any file associated with your child's name and Social Security number.

Equifax
1-888-Equifax (1-888-378-4329)
www.equifax.com

Experian
1-888-397-3742
www.experian.com

TransUnion
1-800-680-7289
www.transunion.com

Shielding Your Credit Report

Credit Freeze FREE

If you're concerned about identity theft, those reported mega-data breaches, or someone gaining access to your credit report without your permission, you might consider placing a credit freeze on your report. This is not a freeze on your credit card, it is only a freeze to your credit report.

Also known as a "security freeze", this tool lets you restrict access to your credit report, which makes it more difficult for identity thieves to open new accounts in your name. Most creditors need to see your credit report before they approve a new account so, if they can't see your file, they may not extend the credit. A credit freeze does not:

- Prevent you from getting your free annual credit report.
- Keep you from opening a new account, applying for a job, renting an apartment, or buying insurance. If you are doing any of these, you will need to lift the freeze temporarily, either for a specific time or for a specific party, say, a potential landlord or employer. The lead times to lift a freeze can vary, so it is best to check with the credit reporting company in advance.
- Prevent a thief from making charges to your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

Fraud Alert FREE

A credit freeze locks down your credit. A fraud alert allows creditors to get a copy of your credit report as long as they take steps to verify your identity. For example, if you provide a telephone number, the business must call you to verify whether you are the person making the credit request. Fraud alerts may be effective at stopping someone from opening new credit accounts in your name, but they may not prevent the misuse of your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

To place a fraud alert on your credit reports, contact one of the nationwide credit reporting companies. A fraud alert is free. You must provide proof of your identity. The company you call must tell the other credit reporting companies; they, in turn, will place an alert on their versions of your report.

NOTES:

Identity Theft Protection Services

If you're concerned about data breaches or identity theft, you may consider signing up for identity theft protection services.

Before you enroll, it's important to weigh the costs and benefits of paid services, and you can also compare them with free and low-cost services. These services charge a fee. Many companies refer to their services as identity theft protection services. No service can protect you from having your personal information stolen. What these companies offer are monitoring and recovery services. Monitoring services watch for signs that an identity thief may be using your personal information. Recovery services help you deal with the effects of identity theft after it happens. Monitoring and recovery services are often sold together, and may include options like regular access to your credit reports or credit scores.

Identity Recovery Services $$$$

These services are designed to help you regain control of your good name and finances after identity theft occurs. Usually, trained counselors assist you with addressing your identity theft problems. They may help you write letters to creditors and debt collectors, place a freeze on your credit report to prevent an identity thief from opening new accounts in your name, or guide you through documents you have to review. Some services will represent you in dealing with creditors or other institutions if you formally grant them authority to act on your behalf.

Identity Theft Insurance $$$$

This is offered by most of the major identity theft protection services. The insurance generally covers only out-of-pocket expenses directly associated with reclaiming your identity. Typically, these expenses are limited to things like postage, copying, and notary costs. Less often, the expenses might include lost wages or legal fees. The insurance generally doesn't reimburse you for any stolen money or financial loss resulting from the theft.

Alternatives to Commercial Identity Theft Protection Services FREE

Here are some low-cost or free ways you can protect yourself against identity theft:

- Monitor your credit reports for free. Federal law requires each of the three major credit reporting agencies to give you a free credit report upon request at least once each year. Visit www.AnnualCreditReport.com, the only government-sponsored website for free credit reports.
- Review statements for your credit card, bank, retirement, brokerage, and other accounts every month—or log in and check them even more often.
- Review the explanation of benefits (EOB) statements you get from your health insurance providers. If you see treatments you never received, immediately tell your insurer and medical providers.

You can regularly monitor your credit ratings and information at

www.AnnualCreditReport.com

Resources

OnGuardOnline.gov has more tips and interactive games to help you be a smarter consumer on issues related to spyware, lottery scams, and other swindles.

You can regularly monitor your credit ratings and information at www.AnnualCreditReport.com.

If your wallet, Social Security number, or other personal information is lost or stolen, there are steps you can take to help protect yourself from identity theft. Visit www.IdentityTheft.gov/Info-Lost-or-Stolen for free personal recovery plans and step-by-step guidance to help identity theft victims recover.

File a fraud report at www.ftc.gov/complaint or call 877-FTC-HELP (877-382-4357). If the fraud relates to medical services or taxes, you may need to also file a police report.

1. Write down three things that you will do differently going forward to protect your identity.

2. Write down three things you will do differently when approached with an offer or when looking for services online.

NOTES:

Proudly presented by

Broadview
Federal Credit Union

700 Patroon Creek Boulevard
Albany, NY 12206
FinancialWellBeing@BroadviewFCU.com

B4400-17 9/2025