

## Protecting Yourself From



## Identity Theft

While no one is safe from identity theft, there are steps you can take to lower your risks. We have compiled this information, advice and resources to help you protect yourself. As you read through this information, remember: Your personal information is only as secure as the least secure way it is stored or disclosed.

### How Identity Theft Can Affect Me or my Loved Ones

Identity theft can damage your finances, credit rating and reputation, and complicate many areas of your life. Identity Thieves might:

- drain your bank account;
- make purchases with your credit cards;
- open new accounts (bank, cell phone, utility, credit card, etc) in your name;

## Identity Theft

Wednesday, 11 May 2016 17:57 - Last Updated Wednesday, 11 May 2016 18:01

---

- get identity and government documents issued with your name and their photos;
- receive medical care under your insurance; take out loans in your name; and/or,
- create a false criminal record for you by using your identifying information when invested or arrested by law enforcement.

There is also a growing threat in this country of unscrupulous people using your Social Security number to :

- file a false tax return and collect a refund; or,
- get a job and have earnings reported as your income.

### **IDENTITY THEFT CAN CREATE MANY DIFFERENT KINDS OF PROBLEMS FOR YOU, SO IT IS IMPORTANT THAT YOU:**

- Ø TAKE PREVENTATIVE MEASURES TO PROTECT YOURSELF AND YOUR FAMILY
- Ø LOOK FOR THE WARNING SIGNS THAT YOUR IDENTITY IS VULNERABLE
- Ø CORRECT ANY PROBLEMS THAT ARISE FROM STOLEN IDENTITY

The most common ways identity thieves obtain other people's personal information is by

stealing it either online or from people's mailboxes and trashcans. Be careful with your personal information. Reduce your chances of ID theft by:

- Getting smart about internet safety and [protecting sensitive information online](#) .
- Opting out of pre-screened offers for credit cards and insurance. Learn more about reducing [junk mail and spam](#) or call 1-888-5-OPTOUT to greatly reduce the amount of mail you receive.
- Keeping necessary documents with sensitive information in a safe place. Never leave items like your social security card in places that are vulnerable to theft such as your wallet or car.
- Shredding any documents that contain sensitive information before disposing of them.
- Employing the help of Identity Monitoring services to help keep you informed of possible identity theft taking place

### **What are identity theft protection services?**

Many companies refer to their services as identity theft protection services. In fact, 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.

### **Monitoring Services**

There are two basic types of monitoring services — credit monitoring and identity monitoring.

Credit monitoring tracks activity on your credit reports at one, two, or all three of the major credit reporting agencies (CRAs) — Equifax, Experian, and TransUnion. If you spot activity that might result from identity theft or a mistake, you can take steps to resolve the problem before it grows. Usually, credit monitoring will alert you when:

## Identity Theft

Wednesday, 11 May 2016 17:57 - Last Updated Wednesday, 11 May 2016 18:01

---

- a company checks your credit history
- a new loan or credit card account is opened in your name
- a creditor or debt collector says your payment is late
- public records show that you've filed for bankruptcy
- there is a legal judgment against you
- your credit limits change
- your personal information, like your name, address, or phone number, changes

Credit monitoring only warns you about activity that shows up on your credit report. But many types of identity theft won't appear. For example, credit monitoring won't tell you if an identity thief withdraws money from your bank account, or uses your Social Security number to file a tax return and collect your refund.

Some services only monitor your credit report at one of the CRAs. So, for example, if your service only monitors TransUnion, you won't be alerted to items that appear on your Equifax or Experian reports. Prices for credit monitoring vary widely, so it pays to shop around.

### **Questions to ask credit monitoring service providers:**

- Which credit reporting agencies do you monitor?

- How often do you monitor CRA reports? Some monitor daily; others are less frequent.
- What access will I have to my credit reports? Can I see my reports at all three CRAs? Is there a limit to how often I can see my reports? Will I be charged a separate fee each time I view a report?
- Are other services included, such as access to my credit score?

Identity monitoring alerts you when your personal information — like your bank account information or Social Security, driver's license, passport, or medical ID number — is being used in ways that generally don't show up on your credit report. For example, identity monitoring services may tell you when your information shows up in:

- change of address requests
- court or arrest records
- orders for new utility, cable, or wireless services
- payday loan applications
- check cashing requests
- social media

- websites that identity thieves use to trade stolen information

To find out if your information is being misused, identity monitoring services must check databases that collect different types of information to see if they contain new or inaccurate information about you. For example, they might check the National Change of Address database to see if anyone is trying to redirect your mail. The effectiveness of the monitoring will depend on factors like the kinds of databases the service checks, how good the databases are at collecting information, and how often the service checks each database. There also may be information that a service cannot monitor. For example, most monitoring services can't alert you to tax or government benefits fraud, including Medicare, Medicaid, welfare, and Social Security frauds.

### **Questions to ask identity monitoring providers:**

- What kinds of information do you check, and how often? For example, does the service check databases that show payday loan applications to see if someone is misusing your information to get a loan?
- What personal information do you need from me and how will you use my information?
- Are other services included with the identity monitoring service? Do they cost extra?

### **Identity recovery services**

Identity recovery services are designed to help you regain control of your good name and finances after identity theft occurs. Usually, trained counselors or case managers walk you through the process of 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**

Identity theft insurance 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.

As with any insurance policy, there may be a deductible, as well as limitations and exclusions. Also, most policies don't pay if your loss is otherwise covered by your homeowner's or renter's insurance. If you're interested in identity theft insurance, ask to see a copy of the company's terms and conditions.

### **Alternatives to commercial identity theft protection services**

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 — at your request — each year. Visit [AnnualCreditReport.com](http://AnnualCreditReport.com) — the only authorized website for free credit reports. If you want to monitor your reports over time, you can spread out your requests, getting one free report every four months.
- Review statements for your credit card, bank, retirement, brokerage, and other accounts every month. Or log in and check them even more frequently. They can tip you to fraudulent charges on your accounts long before issues show up on your credit report.
- 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.

- Consider placing a credit freeze — also known as a security freeze — on your credit files with the major credit bureaus. A credit freeze blocks anyone from accessing your credit reports without your permission. Because potential creditors can't check your files, a credit freeze generally stops identity thieves from opening new accounts in your name.

To freeze your credit files, you'll have to contact each of the CRAs separately. If you opt for a freeze, each time you need to allow a company to check your credit — for example, if you apply for a loan or an apartment — you'll have to unlock your file. The process can take a few days. And, unless you already are an identity theft victim, there may be a fee each time you unfreeze and refreeze your credit. Fees vary based on where you live, but commonly range from \$5 to \$10.

If you want to both freeze your credit and get monitoring services, sign up for the monitoring service before placing the credit freeze. That way, the monitoring service can get access to your credit files. Otherwise, you may not be able to complete the service's account creation process. If you lift the freeze to give the service access, restore it as soon as possible.

- Consider taking advantage of free identity theft protection services that businesses and the government may offer you after a data breach. Check out any company online before enrolling. Some scammers send fake “free” offers to steal your personal information.

If you believe you are an identity theft victim or are at risk of becoming one — possibly because you received a data breach notice or your wallet was lost or stolen — you can place a free, initial 90-day fraud alert on 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 90 days, or remove it at any time.

To place an initial alert, contact one of the three credit reporting agencies. The agency you contact must tell the other two agencies about your alert. You'll get a letter from each CRA confirming that it placed a fraud alert on your file. The letter also will tell you that you are entitled to a free credit report — even if you already ordered your free annual credit report this year — and explain how to request the report. You will have to separately request a free report from each CRA.

### IdentityTheft.gov Offers Free Personal Recovery Plans

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 RobodIdentidad.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

### Cyber threats

While computers and the internet have many positive attributes for society, they also give criminals opportunities to steal your personal information. Cyber criminals have demonstrated their ability to use the latest technologies against us. They are constantly developing new ways to trick and exploit people through their use of the internet. They use malicious software ("known as "malware") to disrupt or hijack your computer with virus and spyware. They secretly install malware programs without your knowledge or consent through email attachments, downloads and links within emails, instant messages or pop-up windows.

Warning signs of malware include:

- Slow or sluggish performance
- Computer crashes
- Repeated error messages
- Being automatically sent to websites you didn't mean to visit
- An unintended reset to a new internet home page that can't be undone
- Getting bombarded with pop-up ads and/or ads popping up when a browser is not open
- Finding a new toolbar added to your browser
- Seeing new icons on your desktop
- Your online search result pages only show ads

Mobile Device malware signs include:

- Decreased battery life

- Interrupted or dropped calls
- Crashing apps

### WAYS TO PROTECT YOURSELF

- Carefully read all disclosures, including the privacy statement and licensing agreement, before downloading and installing software (malware might be bundled in with it)
- Look for wording about personal information collection, internet activity monitoring, or additional programs
- If malware is found or suspected:
  - o Immediately stop all online activities that require you to enter any kind of personal information
  - o Update and then run your security software
    - o Get reliable technical support if possible.